Linux Netfilter/Iptables

(skripte za izgradnju Linux vatrozida)

Pripremio: Dinko Korunić

Verzija: 1.1, studeni 2004.

Tijekom prezentacije

- ako što **nije jasno** - pitajte!
- ako što **nije točno** - ispravite!
- diskusija je **poželjna** i **produktivna**
- ako je **prebrzo** - tražite da se uspori!
- ako je pak **presporo** i **uspavljuje** vas - lako se ubrza sa sadržajem
- vremena je malo, sadržaja mnogo - zato su neki sadržaji samo ukratko objašnjeni

Ciljevi prezentacije

- osnovne značajke Netfilter paketnog filtera:
  - karakteristike i mogućnosti
  - tipični tok paketa
  - konfiguracija i korištenje
  - kako napraviti više - manipulacija paketima, itd.
- uspješno korištenje Netfiltera
- grafički alati za konfiguraciju
- prostor za diskusiju i iskustva

Potrebno predznanje

- **apsolutno obavezno**
  - osnovna računalna pismenost:
  - datoteke, direktoriji, hijerarhija programa na Linux i Debian Linux sistemima
  - pokretanje, zaustavljanje servisa
- **nužno**
  - instalacija Debian paketa
- **opcionalno**
  - ?

Sadržaj

- dužina trajanja: 225 minuta [5x 45 minuta]
- tip tečaja: isključivo pokazni
- cjeline:
  1. uvod o vatrozidima
  2. mrežna problematika filtriranja
  3. uvod u osnovno korištenje Netfiltera
  4. napredno korištenje Netfiltera
  5. literatura
  6. diskusija

Uvod u vatrozide

što, zašto, kako, gdje, čime

Što je vatrozid?

- softverski - računalo
- hardverski - crna kutija (XSentry, PIX)

- zadaća - **zaštita mreže** računala
- kontrola nekog prometa - restrikcije, blokada, dozvole, sigurnosni kriteriji:
  - iz jedne u drugu mrežu
  - lokalno
  - Internet i lokalna mreža

Što nije vatrozid?

- **čaroban** - neće napraviti mrežu apsolutno sigurnom, niti će moći zaštiti od svih tipova napada
- **svemoguć** - niz ograničenja, komplicirano je implementirati, dobar vatrozid zahtijeva niz potrošenih sati
- **sveobuhvatan** - tek jedna od točaka zaštite, nužno zaštiti i svako računalo i servis individualno i dodatno

Zašto vatrozid?

- dodatna mrežna **sigurnost**
  - nesigurni, problematični servisi i računala
- **kontrola** mrežnog pristupa
  - sigurnosna politika, selektivne dozvole
- **logiranje**
  - analiziranje ulaznog i izlaznog prometa
  - IDS, statistike, itd
- razno
  - QoS, shaping, promjene paketa

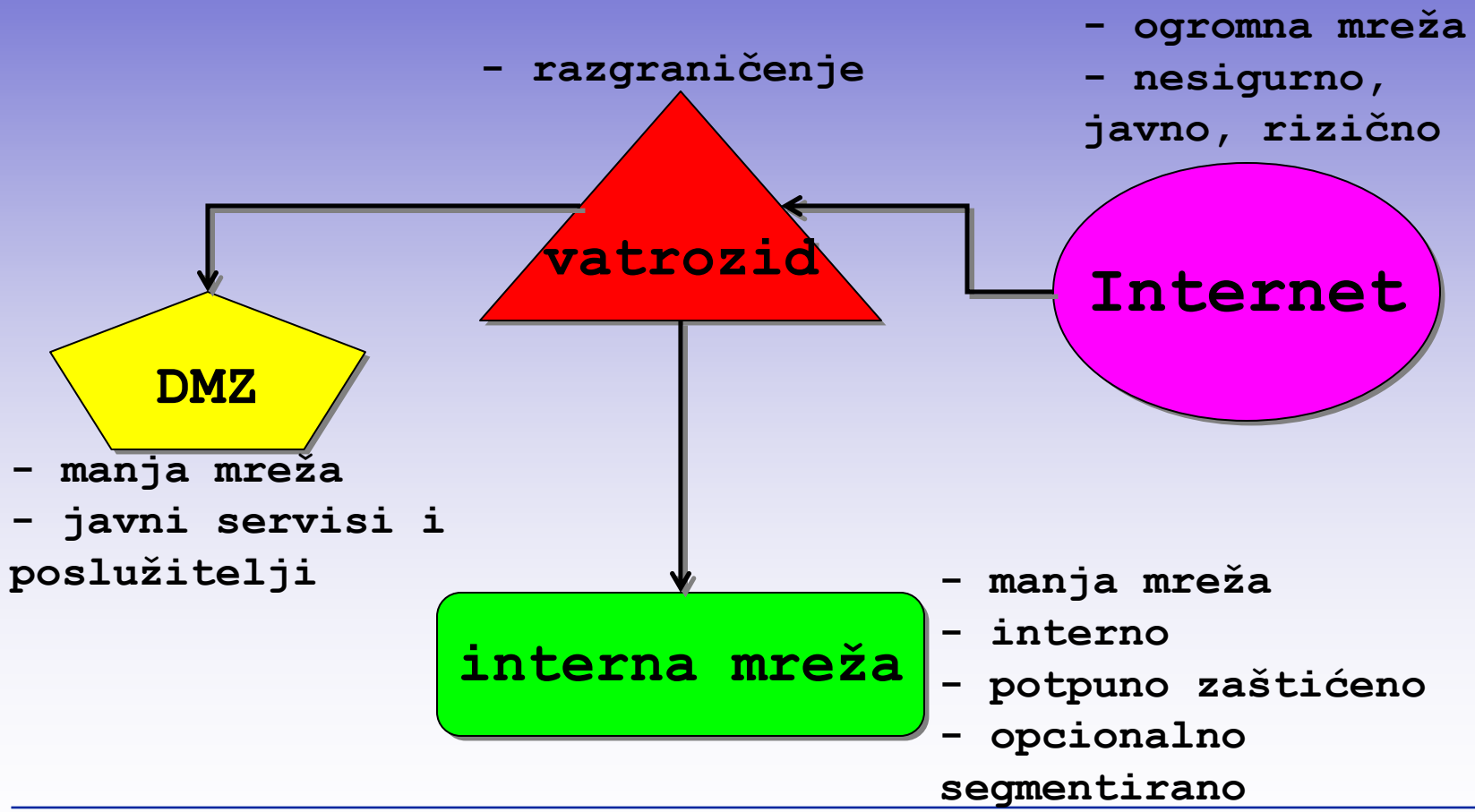
Tipovi vatrozida

- tipovi vatrozida:
  - **proxy**:
    - zahtjevi u ime klijenata
    - Squid
  - **filtrirajući**:
    - prema pravilima se filtriraju paketi (dozvoli, propusti, promijeni, itd)
    - statičko (stateless) i dinamičko filtriranje (stateful)
- moguće imati i oboje!
  - **transparentni** proxy

Filtriranje i mreža

mreža, stanja, filteri, koncepti

Koncepcija mreže



Linux i paketno filtriranje

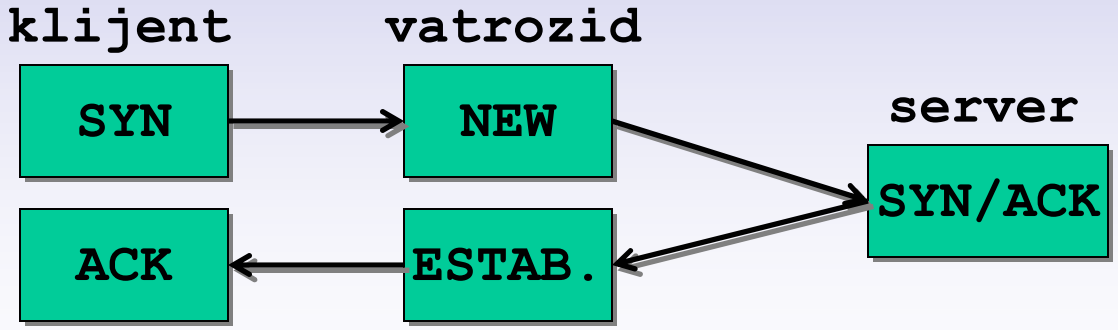
- **Netfilter** - dio 2.4 i 2.6 jezgre (kernel hooks)
- **Iptables** - korisnička aplikacija za upravljanje
- nekada **ipchains** (2.2) i **ipfwadm** (2.0)
- karakteristike:
  - filtriranje paketa, translacija adresa (izvorišnih i odredišnih), translacija portova, mijenjanje paketa
- **paketni filter** - pregledom zaglavlja paketa koji prolaze određuje o budućnosti paketa (odbaci, primi, promijeni)

Filtriranje po stanju

- SPI - Stateful Packet Inspection
- **dinamičko filtriranje** paketa
- prate se **stanja konekcija** kroz vatrozid (connection tracking) i odlučuje se o njihovoj ispravnosti
- SPI pregledava zaglavlja i **sadržaj** paketa radi odluke o paketu
- odluke su bazirane na **kontekstu** koji je određen **proteklim paketima**

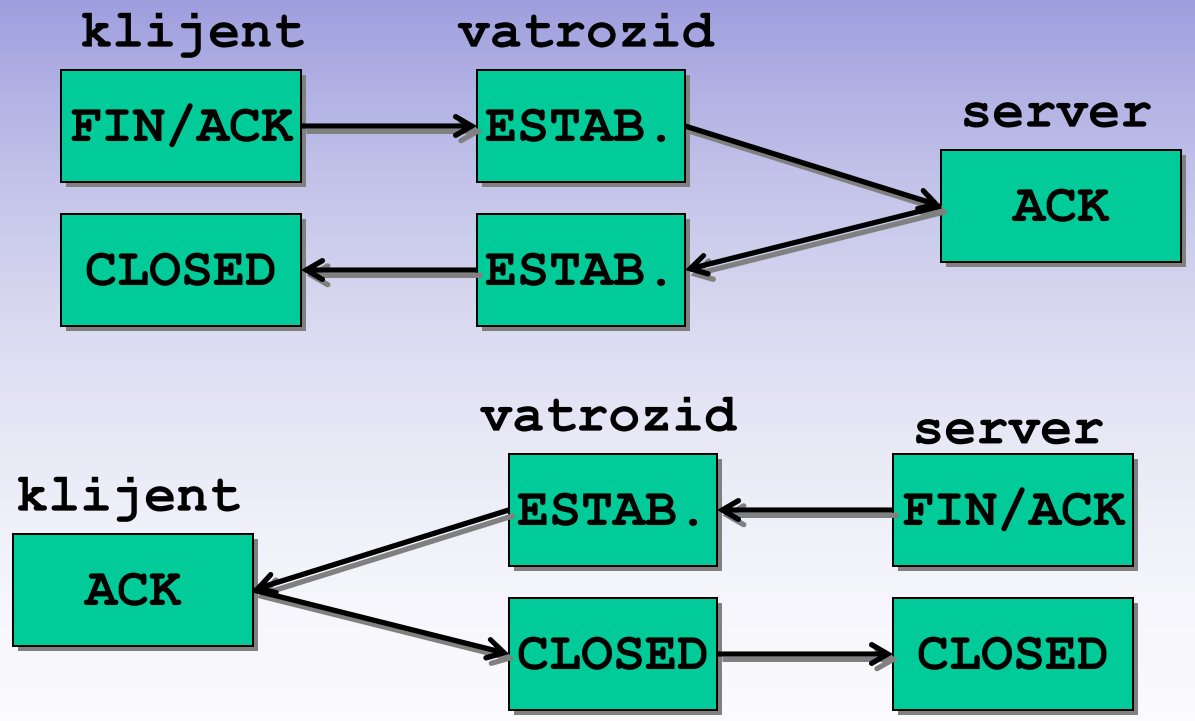
TCP stanja

- RFC 793 - Transmission Control Protocol
- TCP konekcija
  - nastaje kao "rukovanje" u tri smjera
  - sesija počinje sa SYN, zatim SYN/ACK i naposljetku ACK za uspješno ostvarenje:



TCP stanja (2)

– zatvaranje konekcije - rukovanje u 4 smjera:



Ilegalni paketi (1)

- SYN/FIN:
  - SYN za iniciranje konekcije, ne može imati ni FIN ni RST flag
  - ostale loše" kombinacije: SYN/FIN/PSH, SYN/FIN/RST, SYN/FIN/RST/PSH
- FIN
  - bez ACK, a inače je nužno slati ACK za prekidanje postojeće konekcije
- NULL (bez zastavica)
- itd.

Ilegalni paketi (2)

- TCP connect scan:
  - potpuno rukovanje, lako otkriti
- TCP SYN scan:
  - prekinuto rukovanje, vraća RST/ACK (zatvoren) ili ACK (otvoren port), odgovor RST/ACK
- TCP FIN scan:
  - RST kao odgovor za zatvoreni port
- TCP Xmas Tree scan:
  - FIN, URG i PUSH, RST kao odgovor ako je zatvoren port

Ilegalni paketi (3)

- TCP NULL scan:
  - NULL odlazno, RST dolazno ako je port zatvoren
- UDP scan:
  - UDP paket, dolazi ICMP Port Unreachable ako je zatvoren
- stack fingerprint
- najčešći scanneri:
  - Nmap, Saint, Strobe, Nessus (integracija sa Nmap), Queso, itd.

Fragmentiranje

- paket veći od TCP **MSS** (Maximum Segment Size) ili **MTU** (Maximum Tranmission Unit)
- nužno fragmentiranje - da bi paket došao do odredišta
- samo **prvi** fragment sadržava zaglavlje
- **analiza** tek nakon spajanja fragmenata
- podložno napadima:
  - preklapanje podataka tako da prepišu zaglavlje
  - fragmentacijski DoS i DDoS

NAT (1)

- Network Address Translation, Network masquerading, IP masquerading
- **prepisivanje** IP adresa paketa koji prolaze
- često se koristi zbog **manjka** IPv4 adresa
- nedostatci:
  - **ne rade** svi Internet protokoli
  - nema **end-to-end** spojenosti (nije direktno)
  - nužna **dodatna** podrška u vatrozidu za neke više protokole (Application Layer Gateways - ALG)

NAT (2)

- tipovi NAT:
  - **NAPT**: NAT koristeći mapiranje portova, omogućava više strojeva da imaju jednu IP adresu
    - **SNAT**: prepisuje IP računala koje je iniciralo konekciju
    - **DNAT**: prepisuje IP odredišnog računala
  - **statički** NAT: samo prepisivanje adrese, a ne i mapiranje portova; nova IP adresa za svaku pojedini vanjski spoj

NAT (3)

- MASQUERADING:
  - više računala koristi spoj na Internet **transparentno** kroz jednu IP adresu
  - transparentno se **mijenja** SA paketa na eksternu adresu i kroz **conntrack** pamte podatci
  - pri povratku odgovora-paketa, kroz conntrack podatke odlučuje kome **proslijediti** paket
  - benefit: korištenje samo 1 IP adrese, **sigurnost**
  - problem: UDP (potrebna posebna podrška), TCP **iniciran izvana** (FTP), load balancing, failover

Netfilter - početnica

početni koraci

put paketa

Zašto Netfilter?

- filtriranje **po stanju** - connection tracking
- automatsko **defragmentiranje**
- napredno **matchiranje**:
  - rate limit, podatci u paketu, itd.
- napredno **logiranje**
- **zahvati** nad paketima
  - nad podatcima u paketu
- **userland** pristup paketima
- port **forwarding**

Kako do Netfiltera

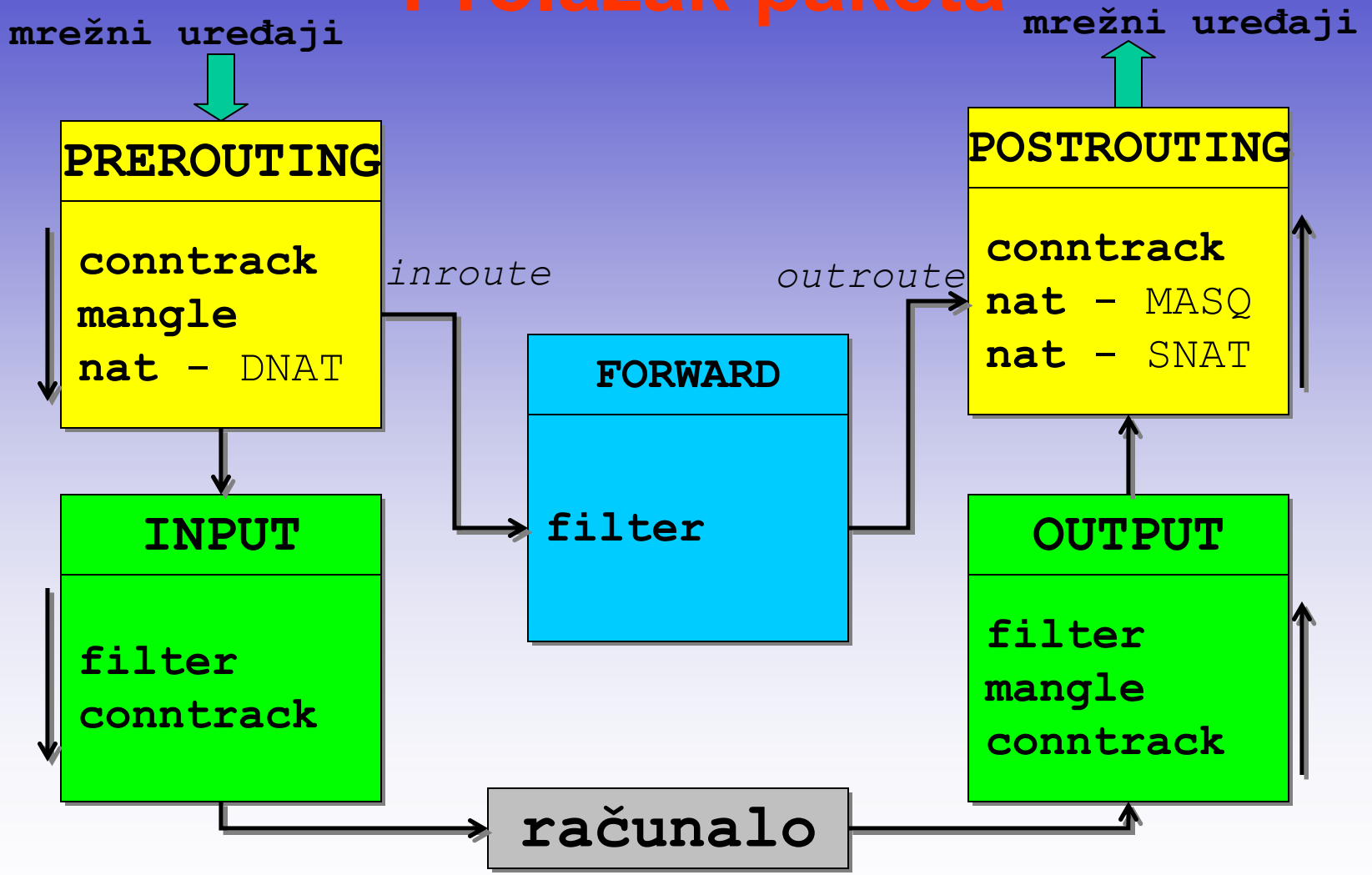
- *uradi-sam*
  - *kernel: CONFIG_IP_NF**
  - *iptables - Debian paket*
  - *Patch-O-Matic!*

- **CARNet paketi**:
  - kernel-cn - ima većinu ugrađenu
  - iptables-cn - ima dodatke (stealth modul)

Osnovni pojmovi Netfiltera

- **table -** tablice određenih tipova pravila
  - standardno: **filter**, **nat**, **mangle**, **drop**
- **chain -** staza, lanac kroz koju paket prolazi
  - tablice imaju ugrađene lance, moguće i dodati vlastite; lanac = lista pravila!
  - paket koji prolazi kroz ugrađeni lanac biva na kraju propušten (**accept**) ili odbačen (**drop**)
  - paket koji ne pogodi niti jedno pravilo u dodatnom lancu biva vraćen u "pozivajući" lanac
- **rule -** pravila u tablicama/lancima

Prolazak paketa



Prolazak paketa (2)

- kad se odlučuje o **sudbini** paketa:
  - unutar INPUT, FORWARD, OUTPUT lanaca

- put paketa:
  - sa mrežne kartice u jezgru - gleda se odredište paketa (routing)
  - ako je za računalo, paket ide u **INPUT** lanac
    - ako prođe, procesi koji ga čekaju ga prime

Prolazak paketa (3)

- put paketa...
  - ako nije za računalo i nema prosljeđivanja, odbacuje se; inače se paket prosljeđuje i odlazi u **FORWARD** lanac
  - ako prođe uspješno kroz FORWARD lanac i biva prihvaćen, šalje se dalje
  - takvi paketi za izlaz prolaze kroz **OUTPUT** lanac - ako je i tamo prihvaćen, šalje se kroz odgovarajući uređaj

Korištenje lanaca

- **stvaranje**: `iptables -N ime-lanca`
- **brisanje praznog** vlastitog (ili svih):
  `iptables -X [lanac]`
- **mijenjanje** politike (ugrađeni lanac):
  `iptables -P [lanac] DROP/ACCEPT`
- **listanje** pravila u lancu:
  `iptables -L [lanac]`
- **brisanje** pravila u lancu:
  `iptables -F [lanac]`

Ugrađeni lanci

- ugrađeni lanci u pojedinim tablicama
  - **filter** tablica (osnovno filtriranje):
    - INPUT, FORWARD, OUTPUT
  - **nat** tablica (NAT, MASQ i varijante):
    - PREROUTING, POSTROUTING, OUTPUT
  - **mangle** tablica (promjene paketa):
    - PREROUTING, OUTPUT

Korištenje pravila (1)

nužno je specificirati u svakom pravilu:

- **tablicu**: -t tablica
- **operaciju** nad nekim lancem:
  - dodavanje: -A
  - brisanje: -D
  - zamjena: -R
  - ubacivanje: -I
- **uzorak**
- **akcije nad paketom**

Korištenje pravila (2)

- **uzorak** za poduzimanje akcije:
  - protokol (TCP, UDP, ICMP, ...):- p
  - izvorišna adresa:- s
  - odredišna adresa:- d
  - ulazni uređaj:- i
  - izlazni uređaj:- o
  - drugi i ostali fragmenti paketa:-- fragment
  - odredišni port:-- dport
  - izvorišni port:-- sport
  - TCP zastavice:-- tcp flags

Korištenje pravila (3)

- **uzorak**..
  - stanje paketa (NEW, ESTABLISHED, RELATED, INVALID): --state
  - izvorišna MAC adresa: --mac-source
  - TOS bitovi u paketu: --tos
  - limit brzine ulaza paketa: --limit
  - limit max brzine ulaza: --limit-burst
  - vlasnik paketa po UID: --uid-owner userid
  - vlasnik paketa po GID: --gid-owner groupid
  - itd...

Korištenje pravila (4)

- **akcije nad** s paketom:
  - prihvatiti: ACCEPT
  - tiho odbaciti: DROP
  - odbaciti i javiti pošiljatelju: REJECT
  - logirati i nastaviti obradu: LOG
  - logirati kroz userland: ULOG
  - zamijeniti SA i DA i ponovno poslati: MIRROR
  - nahraniti paket u userland: QUEUE
  - vratiti u prethodni lanac: RETURN
  - poslati u neki drugi lanac

Osnovna upotreba

```
iptables -A INPUT -s !
  161.53.71.0/255.255.255.0 -i eth0 -p
  udp -m udp --dport 135:139 -j DROP
iptables -A INPUT -s 161.53.2.70 -p udp
  -m udp --dport 123 -j ACCEPT
iptables -A INPUT -s ! 161.53.71.235 -i
  eth0 -p tcp -m tcp --dport 873 -j
  DROP
iptables -A INPUT -s 161.53.71.194 -p
  tcp -m tcp --dport 3632 -j ACCEPT
```

Netfilter - napredno korištenje

dinamičko, zaštite, ideje

filtriranje, prosljeđivanje, p2p, tos, ttl
ipv6, tipični napadi, itd.

SPI kroz primjer (1)

- brzo i jednostavno do SPI
- opcionalno učitati module:

```
modprobe ip_conntrack
modprobe ip_conntrack_ftp
```

- primijeniti standardnu politiku na ugrađene lance:

```
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT ACCEPT
```

SPI kroz primjer (2)

- stvaramo state_chk lanac
- blokiranje svih dolaznih konekcija osim onih koje mi ne iniciramo:

```
iptables -N state_chk
iptables -A state_chk -m state --state
  ESTABLISHED,RELATED -j ACCEPT
iptables -A state_chk -m state --state
  NEW -i ! eth0 -j ACCEPT
iptables -A state_chk -j DROP
```

SPI kroz primjer (3)

- ubaci lanac u input i forward lance:

```
iptables -A INPUT -j state_chk
iptables -A FORWARD -j state_chk
```

- **VAŽNO!**
  - ako se koristi IP forwarding, nužno upaliti u jezgri (ili kroz /etc/sysctl.conf):

```
sysctl -w net/ipv4/ip_forward=1
```

SPI - stanja (1)

- nastavak priče o SPI
- NEW
  - **prvi paket** kojeg conntrack vidi u specifičnoj konekciji
  - najčešće prvi SYN paket, ali ne nužno
- ESTABLISHED
  - ima **već viđenog** prometa u oba smjera
  - host pošalje podatak i primi kasnije odgovor (na odgovor NEW postaje ESTABLISHED)

SPI - stanja (2)

- RELATED
  - **konekcija** koja se odnosi na **već postojeću** (ESTABLISHED), nastaje izvan glavne postojeće konekcije
  - npr. FTP-data (REL) i FTP-ctrl (EST)
  - npr. ICMP odgovori, DCC, itd.
- INVALID
  - **neidentificirani** paket, **nepoznatog** stanja

NAT i filtriranje

- funkcionira dobro zajedno
- **maskerada** za uređaj ppp0:

```
iptables -t nat -A POSTROUTING -o ppp0
  -j MASQUERADE
```

- zabrani određene ulazne ili forwardane pakete iz ppp0 uređaja:

```
iptables -A INPUT -i ppp0 -m state --
  state NEW,INVALID -j DROP
iptables -A FORWARD -i ppp0 -m state --
  state NEW,INVALID -j DROP
```

Statički NAT

- ručna **statička** pravila:

```
iptables -A PREROUTING -s
  161.53.71.0/255.255.255.0 -d
  161.53.71.235 -i eth0 -p udp -m udp -
  -dport 53 -j DNAT --to-destination
  161.53.71.178
iptables -A PREROUTING -d 161.53.71.248
  -j DNAT --to-destination 192.168.0.10
iptables -A POSTROUTING -s 192.168.0.10
  -j SNAT --to-source 161.53.71.248
```

Prosljeđivanje portova

- obavlja se u 2 koraka:
  - **DNAT** paketa

```
iptables -t nat -A PREROUTING -i
eth0 -p proto -d orig_ipaddr_eth0 -
-dport orig_port -j DNAT --to
dest_ipaddr:dest_port
```

  - **forwardiranje** dotičnih NAT-anih paketa:

```
iptables -A FORWARD -i eth0 -o eth1
-p proto -d dest_ipaddr --dport
dest_port -j ACCEPT
```

Filtriranje stringova

- pregled sadržaja paketa
  - npr. "/default.ida? .exe?/c+dir"
  - zahtjevno!

```
iptables -A INPUT -i eth_if -p tcp --dport
  string_dest_port -m state --state
  ESTABLISHED -m limit --limit 1/h -m string -
  -string "char_string" -j LOG --log-level
  notice --log-prefix "REJECT char_string"
iptables -A INPUT -i eth_if -p tcp --dport
  string_dest_port -m state --state
  ESTABLISHED -m string --string "char_string"
  -j REJECT --reject-with tcp-reset
```

Filtriranje P2P alata (1)

- **Gnutella**:

```
iptables -A (CHAIN) -p TCP -m string --string
  "GNUTELLA CONNECT/" -j DROP
iptables -A (CHAIN) -p TCP -m string --string
  "urn:sha1:" -j DROP
iptables -A (CHAIN) -p TCP -m string --string
  "GET /get/" -j DROP
iptables -A (CHAIN) -p TCP -m string --string
  "GET /uri-res/" -j DROP
iptables -A (CHAIN) -p TCP --dport 80 -m string -
  -string "GET /gcache" -j DROP
iptables -A (CHAIN) -p TCP --dport 80 -m string -
  -string "/gcache.php" -j DROP
```

Filtriranje P2P alata (2)

- **BitTorrent**:

```
iptables -A (CHAIN) -p TCP -m string --string
  "BitTorrent protocol" -j REJECT --reject-
  with tcp-reset
```

- **FastTrack** (**KaZaA**, **Grokster**, **IMesh**, itd)

```
iptables -A (CHAIN) -p TCP -m string --string
  "X-Kazaa-" -j REJECT --reject-with tcp-reset
iptables -A (CHAIN) -p UDP -m string --string
  "KaZaA" -j DROP
iptables -A (CHAIN) -p UDP -m string --string
  "fileshare" -j DROP
```

Filtriranje P2P alata (3)

- **SoulSeek**:

```
iptables -A (CHAIN) -d server.slsk.org -j DROP
```

- **MP2P** (Blubster/Piolet):

```
iptables -A (CHAIN) -p TCP -d 128.121.0.0/16 -
  -dport 80 -m string --string "GET /gateway/"
  -j DROP
```

- **FileNavigator/Swapptor**:

```
iptables -A (CHAIN) -d cache.filenavigator.com
  -j DROP
```

- **WinMX**, **FileShare**, **DirectConnect**
  - nužno blokirati koristeći IP servera, hubova, itd.

Transparentni proxy

- Squid - kao **akcelerator**:

```
httpd_accel_host virtual
httpd_accel_port 80
httpd_accel_with_proxy on
httpd_accel_uses_host_header on
```

- **preusmjeravanje** HTTP (tcp/80):

```
iptables -A PREROUTING -i eth1 -p tcp -m tcp -
  -dport 80 -j REDIRECT --to-ports 8080
```

- **ostali** promet:

```
iptables -A POSTROUTING -s
  10.0.0.0/255.255.255.0 -j MASQUERADE
```

Ograničenje protoka

- brzina prihvaćanja paketa - **antiflood**:

```
iptables -N FLOOD
iptables -A FLOOD -p tcp --syn -m limit
  --limit 2/s -j RETURN
iptables -A FLOOD -p tcp --tcp-flags
  SYN,ACK,FIN,RST RST -m limit --limit
  2/s -j RETURN
iptables -A FLOOD -p tcp -j DROP
iptables -A INPUT -p tcp -m state --
  state NEW -j FLOOD
```

Promjene paketa - TOS (1)

- **TOS** (Type Of Service) podešenja - RFC 1060/1349
  - određuje kako se paket tretira kroz mrežu
  - nužna podrška daljnje mrežne opreme
  - 0x00 = Normal-Service, 0x02 = Minimize-Cost, 0x04 = Maximize-Reliability, 0x08 = Maximize-Throughput, 0x10 = Minimize-Delay

```
iptables -t mangle -A PREROUTING -p tcp -m
  multiport --dports https -j TOS --set-
  tos Maximize-Reliability
iptables -t mangle -A PREROUTING -p tcp -m
  multiport --dports ftp-data,www -j TOS -
  -set-tos Maximize-Throughput
```

Promjene paketa - TOS (2)

```
iptables -t mangle -A PREROUTING -p tcp -m
  multiport --dports ssh,ftp,telnet -j TOS
  --set-tos Minimize-Delay
iptables -t mangle -A PREROUTING -p udp -m
  multiport --dports snmp,domain -j TOS --
  set-tos Maximize-Reliability
iptables -t mangle -A PREROUTING -p tcp -m
  multiport --dports smtp -j TOS --set-tos
  Minimize-Cost
iptables -t mangle -A PREROUTING -p icmp -
  j TOS --set-tos Minimize-Delay
```

Logiranje (1)

- kernel - **sysklogd**
  - log leveli - moguće filtrirati logove
  - moguć DoS na sustav ako se sve logira - OPREZ!

```
iptables -t filter -A LDROP -p tcp -m limit --limit
  2/s -j LOG --log-level 6 --log-prefix "TCP drop"
iptables -t filter -A LDROP -p udp -m limit --limit
  2/s -j LOG --log-level 6 --log-prefix "UDP drop"
iptables -t filter -A LDROP -p icmp -m limit --limit
  2/s -j LOG --log-level 6 --log-prefix "ICMP drop"
iptables -t filter -A LDROP -f -m limit --limit 2/s
  -j LOG --log-level 4 --log-prefix "FRAG drop"
iptables -t filter -A LDROP -j DROP
```

Logiranje (1)

- **userspace**:

```
iptables -t filter -A ULDROP -p tcp -m limit --limit
  2/s -j ULOG --ulog-nlgroup 1 --ulog-prefix
  LDROP_TCP
iptables -t filter -A ULDROP -p udp -m limit --limit
  2/s -j ULOG --ulog-nlgroup 1 --ulog-prefix
  LDROP_UDP
iptables -t filter -A ULDROP -p icmp -m limit --
  limit 2/s -j ULOG --ulog-nlgroup 1 --ulog-prefix
  LDROP_ICMP
iptables -t filter -A ULDROP -f -m limit --limit 2/s
  -j ULOG --ulog-nlgroup 1 --ulog-prefix LDROP_FRAG
iptables -t filter -A ULDROP -j DROP
```

Različite korisne postavke (1)

- MSS - postavlja **MSS** paketa da se izbjegnu **MTU** problemi (ICMP Fragmentation Needed):

```
iptables -I FORWARD 1 -p tcp --tcp-
  flags SYN,RST SYN -j TCPMSS --clamp-
  mss-to-pmtu
```

- **Smurf/Fraggle** DDoS (directed broadcast, moguće pojačanje):

```
iptables -A BASIC -i wan_eth -d
  255.255.255.255 -j DROP
iptables -A BASIC -i wan_eth -d
  wan_eth_bcast -j DROP
```

Različite korisne postavke (2)

- **novi** paketi, ali bez SYN:

```
iptables -A BASIC -m state --state
  INVALID -j DROP
iptables -A BASIC -i wan_eth -p tcp ! -
  -syn -m state --state NEW -j DROP
```

- odbacivanje **fragmentiranih** paketa (Teardrop, Bonk):

```
iptables -A BASIC -i wan_eth -f -j DROP
```

- **forward paketa**:

```
echo 1 > /proc/sys/net/ipv4/ip_forward
```

Različite korisne postavke (3)

- odbacivanje **spoofanih** paketa:

```
iptables -A BASIC -i wan_eth -s wan_ip -j DROP
iptables -A BASIC -s 127.0.0.0/255.0.0.0 -i ! lo
  -j DROP
iptables -A BASIC -i wan_eth -d local_lan -j DROP
```

- dozvoli **postojeće** konekcije (opcionalno dodati i FORWARD lanac):

```
iptables -I INPUT 1 -m state --state
  ESTABLISHED,RELATED -j ACCEPT
iptables -I OUTPUT 1 -m state --state
  ESTABLISHED,RELATED -j ACCEPT
```

Različite korisne postavke (4)

- razni "**loši**" paketi:

```
iptables -A INPUT -i eth_wan -m unclean
  -j DROP
```

- **limit novih** konekcija:

```
iptables -A INPUT -i eth_wan -p tcp --
  syn --dport dest_port -m connlimit --
  connlimit-above 2 -j DROP
iptables -A INPUT -i eth_wan -p tcp --
  syn -m state --state NEW -m limit --
  limit 2/s --dport dest_port -j ACCEPT
```

Različite korisne postavke (5)

- postavljanje **TTL** (Time To Live) odlaznih paketa
  - ograničava se put do klijenata, za npr. DNS:

```
iptables -t mangle -o eth_wan -A OUTPUT
  -j TTL --ttl-set 64
```

  - moguće napraviti vatrozid **nevidljivim** za traceroute (poveća se TTL određenim paketima):

```
iptables -t mangle -A PREROUTING -p TCP
  --dport 33434:33542 -j TTL --ttl-inc
  1
```

Različite korisne postavke (6)

- **SYN flood** (nužno povećati conn queue i smanjiti conn establish vrijeme):

```
iptables -A FORWARD -p tcp --syn -m
  limit --limit 1/s -j ACCEPT
```

- ICMP flood - **Ping of Death**:

```
iptables -A FORWARD -p icmp --icmp-type
  echo-request -m limit --limit 1/s -j
  ACCEPT
```

Ilegalne mreže

- ilegalne mreže:
  - **broadcast**: 255.255.255.255/32
  - **loopback**: 127.0.0.0/8
  - link **local**: 169.254.0.0/16
  - **unallocated**: 248.0.0.0/5
  - **test** net: 192.0.2.0/24
  - RFC 1918 class A, B, C **private**: 10.0.0.0/8, 172.16.0.0/16, 192.168.0.0/16
  - class D **multicast**: 224.0.0.0/4
  - class E **reserved**: 240.0.0.0/5

```
iptables -A ILLEGAL -i wan_eth -s illegal_addr
  -j DROP
```

Ilegalne TCP zastavice (1)

- protiv **port scanniranja** (nmap i sl):

```
iptables -A INVALID -i wan_eth -p tcp --tcp-flags
  ALL ALL -j DROP
iptables -A INVALID -i wan_eth -p tcp --tcp-flags
  ALL NONE -j DROP
iptables -A INVALID -i wan_eth -p tcp --tcp-flags
  ALL FIN,URG,PSH -j DROP
iptables -A INVALID -i wan_eth -p tcp --tcp-flags
  ALL SYN,RST,ACK,FIN,URG -j DROP
iptables -A INVALID -i wan_eth -p tcp --tcp-flags
  SYN,RST SYN,RST -j DROP
iptables -A INVALID -i wan_eth -p tcp --tcp-flags
  SYN,FIN SYN,FIN -j DROP
```

Ilegalne TCP zastavice (2)

```
iptables -A INVALID -i wan_eth -p tcp --tcp-flags
  FIN,RST FIN,RST -j DROP
iptables -A INVALID -i wan_eth -p tcp --tcp-flags
  ACK,FIN FIN -j DROP
iptables -A INVALID -i wan_eth -p tcp --tcp-flags
  ACK,PSH PSH -j DROP
iptables -A INVALID -i wan_eth -p tcp --tcp-flags
  ACK,URG URG -j DROP
iptables -A INVALID -i wan_eth -p tcp --tcp-
  option 64 -j DROP
iptables -A INVALID -i wan_eth -p tcp --tcp-
  option 128 -j DROP
```

ICMP blokiranje (1)

- **ICMP**:
  - ping sweep, nužno kontrolirati ICMP promet
  - 0 = **Echo Reply** - odgovor na Echo Request
  - 3 = Destination Unreachable (ulazno) or Fragmentation Needed (izlazno)
  - 4 = Source Quench - da uspori brzinu slanja
  - 8 = **Echo Request** - zahtjev za ICMP 0 odgovorom
  - 11 = Time Exceeded - za traceroute (TTL) i za fragmentirane pakete
  - 12 = Parameter Problem - greška ili problemi sa zaglavljem paketa

ICMP blokiranje (2)

```
iptables -A ICMP -i wan_eth -p ICMP --icmp-
  type 0 -j ACCEPT
iptables -A ICMP -i wan_eth -p ICMP --icmp-
  type 3 -j ACCEPT
iptables -A ICMP -i wan_eth -p ICMP --icmp-
  type 4 -j ACCEPT
iptables -A ICMP -i wan_eth -p ICMP --icmp-
  type 8 -m limit --limit 6/m -j ACCEPT
iptables -A ICMP -i wan_eth -p ICMP --icmp-
  type 11 -j ACCEPT
iptables -A ICMP -i wan_eth -p ICMP --icmp-
  type 12 -j ACCEPT
```

Markiranje paketa

- **označavanje** paketa
  - isključivo lokalno!
  - za QoS, routing, itd.
  - nužno vratiti u chain radi daljnjeg procesiranja!

```
iptables -A PREROUTING -p tcp -m multiport --
  sports 22,107,992,994,53 -j MARK --set-mark 0x1
iptables -A PREROUTING -p tcp -m multiport --
  sports 22,107,992,994,53 -j RETURN
iptables -A PREROUTING -p tcp -m tcp --sport
  8000:8080 -j MARK --set-mark 0x2
iptables -A PREROUTING -p tcp -m tcp --sport
  8000:8080 -j RETURN
```

IPv6 filtriranje

- nužno dodavati module kroz Patch-O-Matic
- ip6tables naredba
- IPv6-in-IPv4:

```
iptables -A INPUT -i ppp0 -d
  charon.twibble.org -p ipv6 -j ACCEPT
```

- čisti IPv6:

```
ip6tables -A INPUT -i eth0 -p tcp -s
  3ffe:ffff:100::1/128 --dport 22 -j ACCEPT
ip6tables -A INPUT -p ipv6-icmp --icmpv6-
  type echo-reply -j ACCEPT
```

Što kad Netfilter nije dovoljan

- nf-HiPAC
  - http://sourceforge.net/projects/nf-hipac/
  - performanse
  - iznimno efikasni paketni filter
  - dodatni userland alat
  - dodatni target
  - robusni, brzi paketni filter
  - otporan na DoS i DDoS

Grafički alati

- XPloy
- Shorewall
- M0n0wall
- IPCop

Literatura (1)

- Iptables tutorial
- Netfilter/Iptables FAQ
- Netfilter/Iptables HOWTO's:
  - Networking Concepts HOWTO
  - Packet Filtering HOWTO
  - Netfilter Hacking HOWTO
  - Netfilter Double NAT HOWTO
  - NAT HOWTO
  - Netfilter Extensions HOWTO
- homeLANsecurity
- LinuxGuruz Netfilter Iptables Firewall

Literatura (2)

- **Portal za CARNetove sistem inženjere**:
  - http://sistemac.carnet.hr/syshelp
- **Sigurnosna politika**:
  - http://sistemac.srce.hr/fileadmin/sem/Politika-ustanove_files/frame.htm

Diskusija!