



SVEUČILIŠTE U ZAGREBU



Fakultet
elektrotehnike i
računarstva

Diplomski studij

Sigurnost komunikacija

Ak. godina 2021/2022

Vatrozid
IDS



Creative Commons



- **slobodno smijete:**

- **dijeliti** — umnožavati, distribuirati i javnosti priopćavati djelo
- **remiksirati** — prerađivati djelo



- **pod sljedećim uvjetima:**

- **imenovanje.** Morate priznati i označiti autorstvo djela na način kako je specificirao autor ili davatelj licence (ali ne način koji bi sugerirao da Vi ili Vaše korištenje njegova djela imate njegovu izravnu podršku).
- **nekomercijalno.** Ovo djelo ne smijete koristiti u komercijalne svrhe.
- **dijeli pod istim uvjetima.** Ako ovo djelo izmijenite, preoblikujete ili stvarate koristeći ga, prerađu možete distribuirati samo pod licencom koja je ista ili slična ovoj.



U slučaju daljnjeg korištenja ili distribuiranja morate drugima jasno dati do znanja licencne uvjete ovog djela. Najbolji način da to učinite je linkom na ovu internetsku stranicu. Od svakog od gornjih uvjeta moguće je odstupiti, ako dobijete dopuštenje nositelja autorskog prava. Ništa u ovoj licenci ne narušava ili ograničava autorova moralna prava.

Sadržaj

- Firewall
- IDS

Pregled

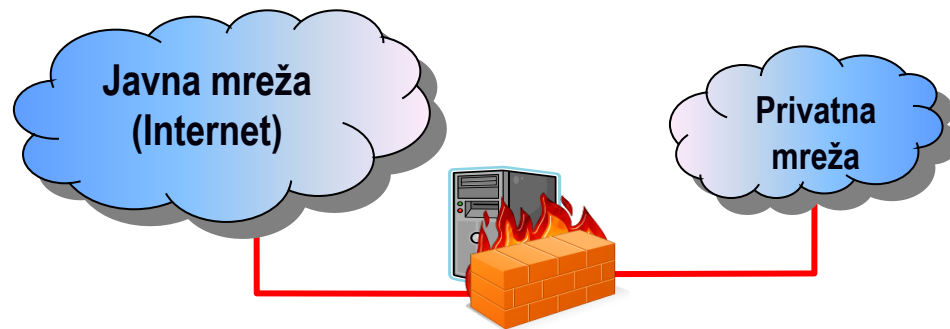
- „Defense in Depth” – sveobuhvatna zaštita
 - perimetar, unutarnja mreža, ljudski faktor
- „Perimeter Security”
 - perimetar - “prednji kraj kružne obrane”
- perimetar uključuje:
 - usmjeritelje
 - **vatrozid** (engl. firewall, sigurnosna stijena)
 - IDS (Intrusion Detection System – sustav za otkrivanje uljeza)
 - VPN (Virtual Private Network)
 - softverska arhitektura
 - DMZ & „Screened Subnet” (oklopljena podmreža)

Zaštita lokalne mreže vatrozidom

- pretpostavka
 - lokalnoj mreži se vjeruje!
 - vanjska mreža je potencijalno opasna
- nezaštićena mreža
 - sigurnost mora biti implementirana na svakom pojedinom računalu
 - jedno ranjivo računalo narušava sigurnost cijele mreže
 - noćna mora administratora!
- zaštićena mreža
 - na granici između vanjske (opasne) i unutarnje (sigurne) mreže postavlja se vatrozid
 - vatrozid omogućava kontrolu pristupa
 - pomaže nadzoru sustava i pojednostavnjuje upravljanje

Firewall – vatrozid, sigurnosna stijena

- mrežni uređaj koji dopušta, zabranjuje ili prosljeđuje mrežne konekcije u skladu sa sigurnosnom politikom
 - hardverski ili softverski
- kontrola prometa između mreža s različitim stupnjevima povjerenja (Internet ↔ privatna lokalna mreža)



Osnovni princip rada vatrozida

- filtriranje paketa (engl. packet filtering) - filtrira promet na različitim slojevima
 - odbacuje ili propušta pakete na temelju:
 - vrste protokola,
 - IP adrese izvorišta / odredišta,
 - brojeva portova,
 - sadržaja datagrama, ...
- posredničke (engl. proxy) usluge
 - programi koji komuniciraju s vanjskim poslužiteljima umjesto internih klijenata
 - 2 komponente: *proxy* poslužitelj i klijent
 - prosljeđuje samo dozvoljene upite

Ograničenja

- nije krajnje rješenje problema sigurnosti
 - ne može u potpunosti nadzirati sadržaj koji se prenosi (virusi – provjeravanje sadržaja paketa, svakodnevno nove vrste virusa)
 - nove vrste napada – novi filteri
 - ne štite od napada unutar mreže (zlonamjerni članovi unutar lokalne mreže)
 - potencijalni problemi s performansama
 - ako je vatrozid kompromitiran mreža postaje nezaštićena
 - „backdoor” u mrežu radi nametnutih restrikcija
- sigurnosne strategije
 - dodijeliti samo nužne (najmanje potrebne) privilegije
 - obrana u dubinu
 - na svim nivoima valja instalirati dodatne sigurnosne zaštite
 - „fail-safe”
 - prestanak rada vatrozida ne smije utjecati na sigurnost sustava

“Thinking About Firewalls”

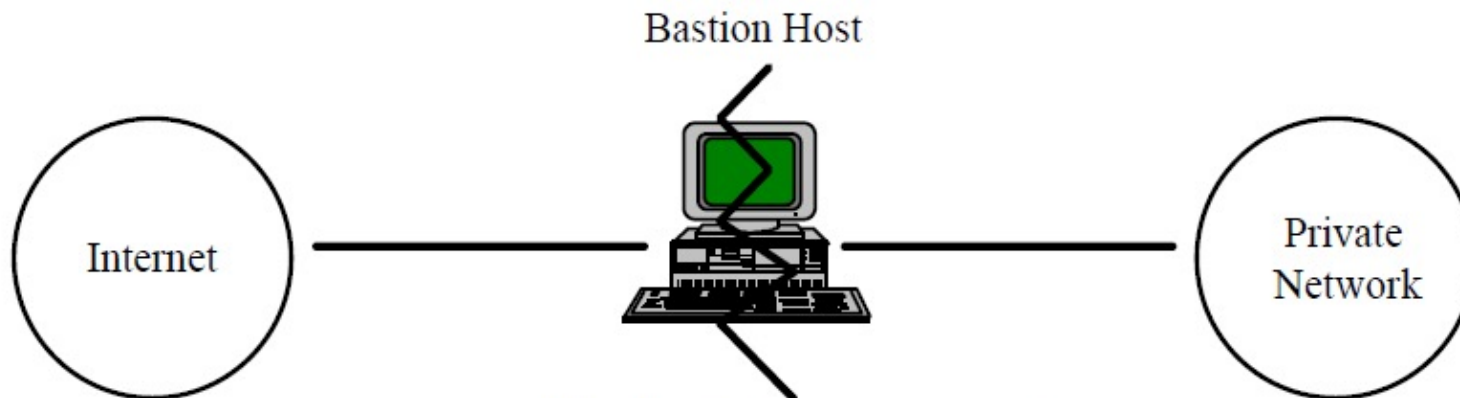
- Marcus J. Ranum, Thinking About Firewalls
 - Trusted Information Systems, Inc., Glenwood, Maryland
 - Proceedings of Second International Conference on Systems and Network Security and Management, SANS II, Washington, DC, 1993

Terminologija

- Screening Router – zaštitni usmjeritelj
 - osnovna komponenta većine vatrozida (ponekad i jedina)
 - usmjeritelj ili računalo koje obavlja usmjeravanje uz mogućnost neke vrste filtriranja paketa
 - posjeduje mogućnost blokiranja prometa između mreža ili određenih računala na nivou IP adresa i portova
- Bastion host
 - bastion, tvrđava, utvrda
 - kritična ali dobro osigurana točka u mreži – redovito kontrolirana, nadzirana, osvježavana, često s modificiranim softverom

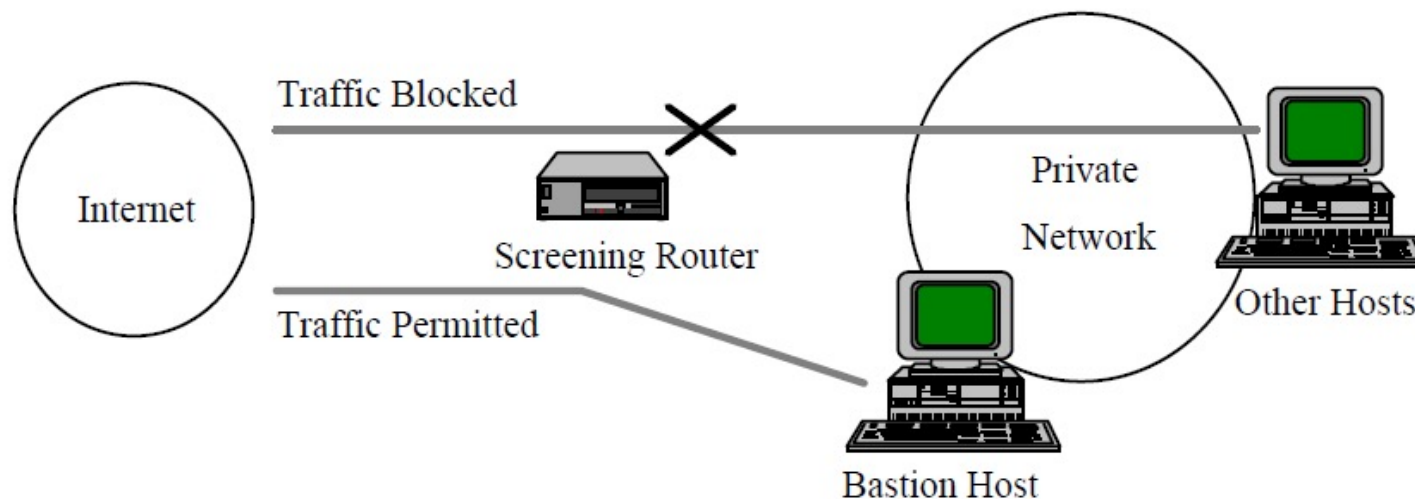
Terminologija

- Dual Homed Gateway
 - umjesto „screening routera” između privatne mreže i Interneta smješta se bastion host
 - onemogućeno prosljeđivanje IP datagrama
 - direktan promet između mreža je onemogućen
 - visoka razina kontrole
 - korištenje usluga preko korisničkih računa na bastion hostu ili posredničkih poslužitelja (proxy)



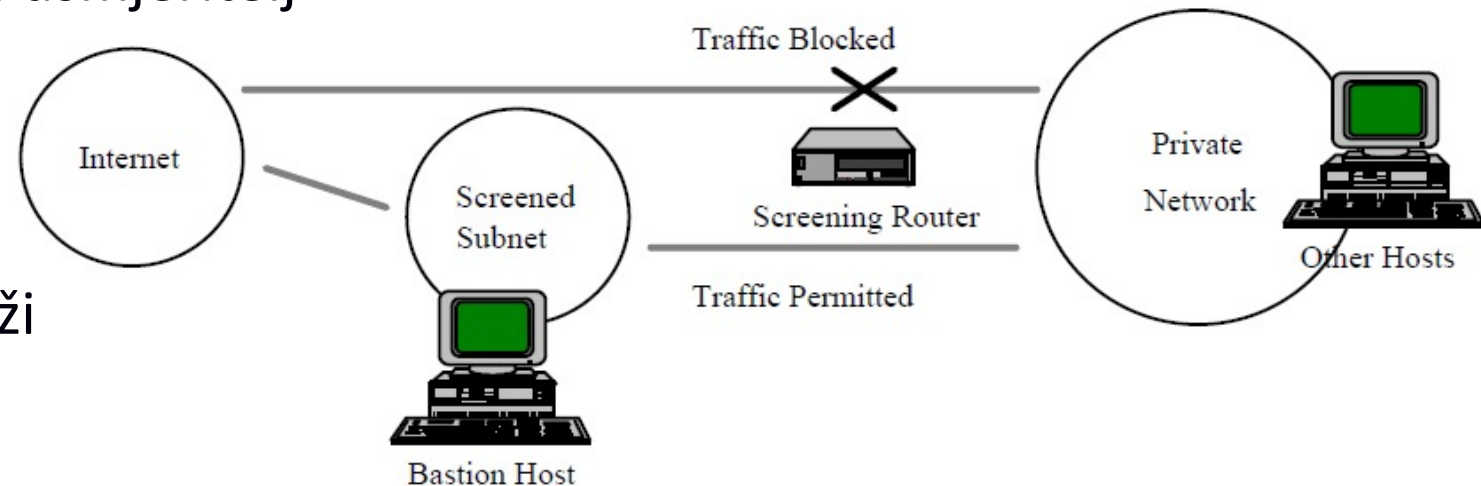
Terminologija

- Screened Host Gateway
 - “screening router” i “bastion host”
 - “bastion host” je u privatnoj mreži i to je jedini sustav dostupan iz javne mreže – visok stupanj sigurnosti
 - omogućen pristup samo malom broju usluga
 - sav ostali promet do lokalne mreže blokiran
 - izlazne konekcije preko proxy poslužitelja



Terminologija

- Screened Subnet
 - izolirana podmreža između Interneta i privatne mreže
 - dozvoljen pristup računalima u podmreži iz javne i iz privatne mreže
 - promet između javne i privatne mreže onemogućen
 - u pravilu unutarnji i vanjski usmjeritelj
 - ne postoji jedinstvena točka koja bi mogla kompromitirati mrežu
 - poželjno ograničiti broj usluga prema lokalnoj mreži
 - u podmreži se u pravilu nalaze bastion hostovi



Terminologija

- DMZ - demilitarizirana zona – engl. „Demilitarized Zone”
 - područje mreže između dva filtera paketa:
 - vanjski filter propušta samo promet izvana
 - interni filter dopušta samo promet iznutra
 - odvaja vanjsku i unutarnju mrežu
 - sadrži računala koja osiguravaju:
 - vanjske usluge (npr. Web poslužitelj, DNS poslužitelj, FTP poslužitelj)
 - *Application gateway* za interne klijente
 - ako je računalo u DMZ kompromitirano:
 - unutarnji promet se ne može snimati - zaštita s internim filterom

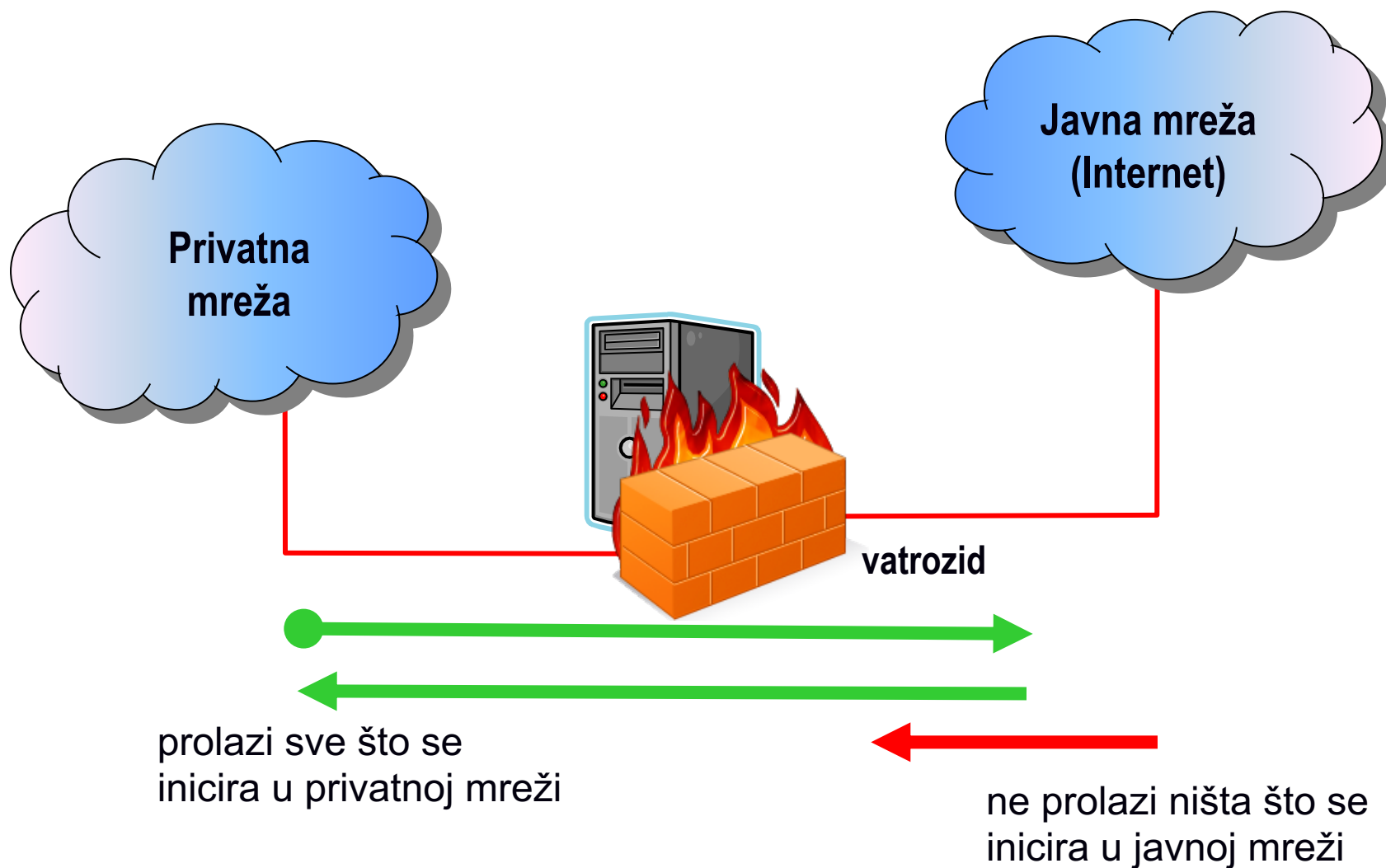
Terminologija

- Application Gateway / Proxy Gateway - posrednik
- interpretira protokol određene aplikacije
 - na primjer HTTP / FTP
 - treba detaljno poznavati aplikacijski protokol
 - za svaki protokol potreban je novi posrednički poslužitelj (proxy)
 - može obavljati napredno filtriranje (na primjer određenih komandi)
- prednosti
 - jeftino
 - velike mogućnosti logiranja
 - unutarnja mreža je nevidljiva
- ograničenja
 - skalabilnost, performanse

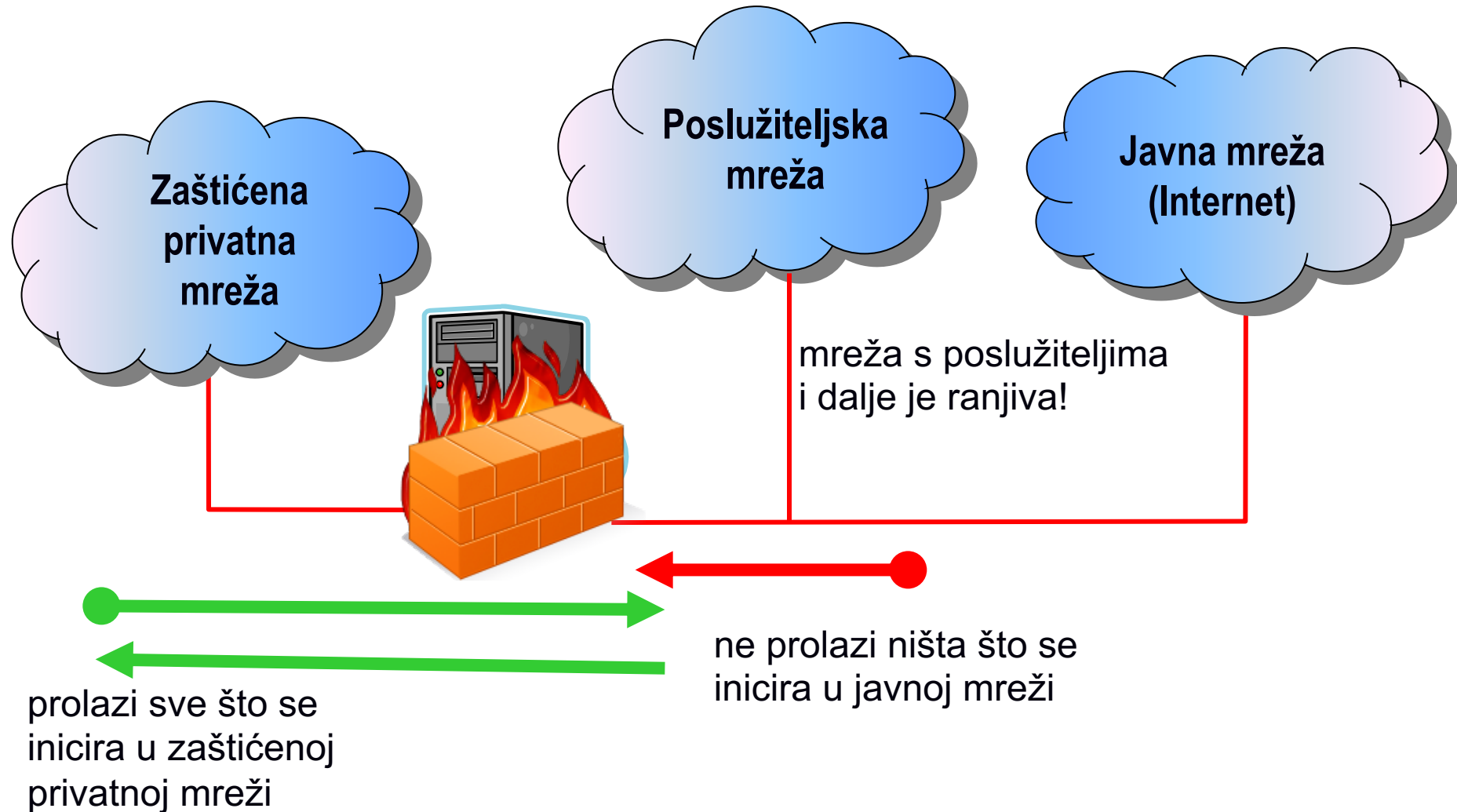
Ostala značajna svojstva vatrozida

- kontrola štete
 - što se događa sa sigurnošću mreže ako je vatrozid kompromitiran ili uništen
- zone rizika
 - kolika je zona rizika u normalnom radu vatrozida - mjera je broj računala ili usmjeritelja koji se vide iz vanjske mreže
- ispad vatrozida
 - može li se lako detektirati: provala, uništenje
 - koliko informacija je sačuvano za naknadnu analizu napada
- jednostavnost korištenja (mreže)
- izvedba
 - zabranjeno je sve što nije izrijeком dozvoljeno
 - dozvoljeno je sve što nije izrijeком zabranjeno

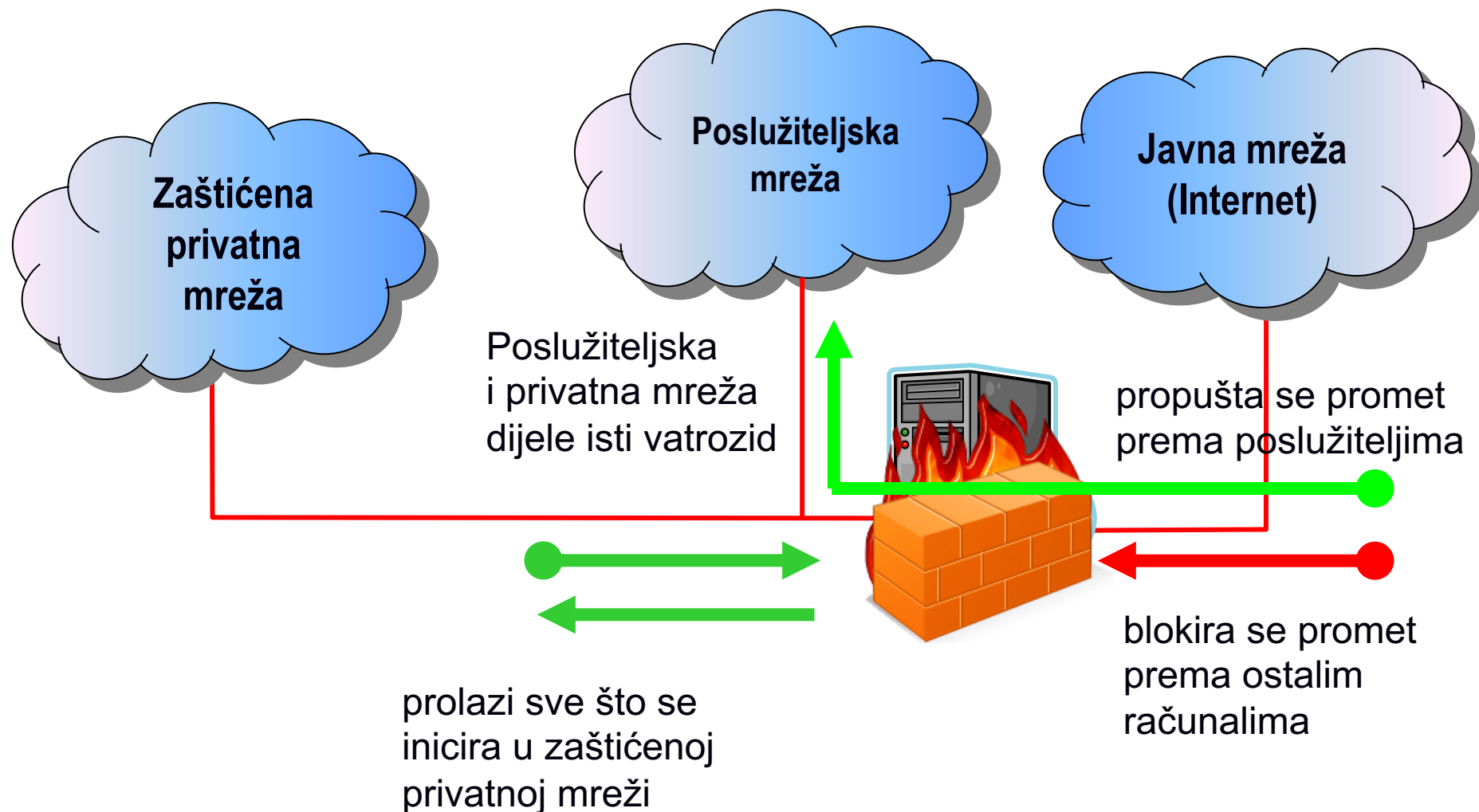
Privatne mreže bez usluga vanjskim korisnicima



Privatne mreže s uslugama za vanjske korisnike

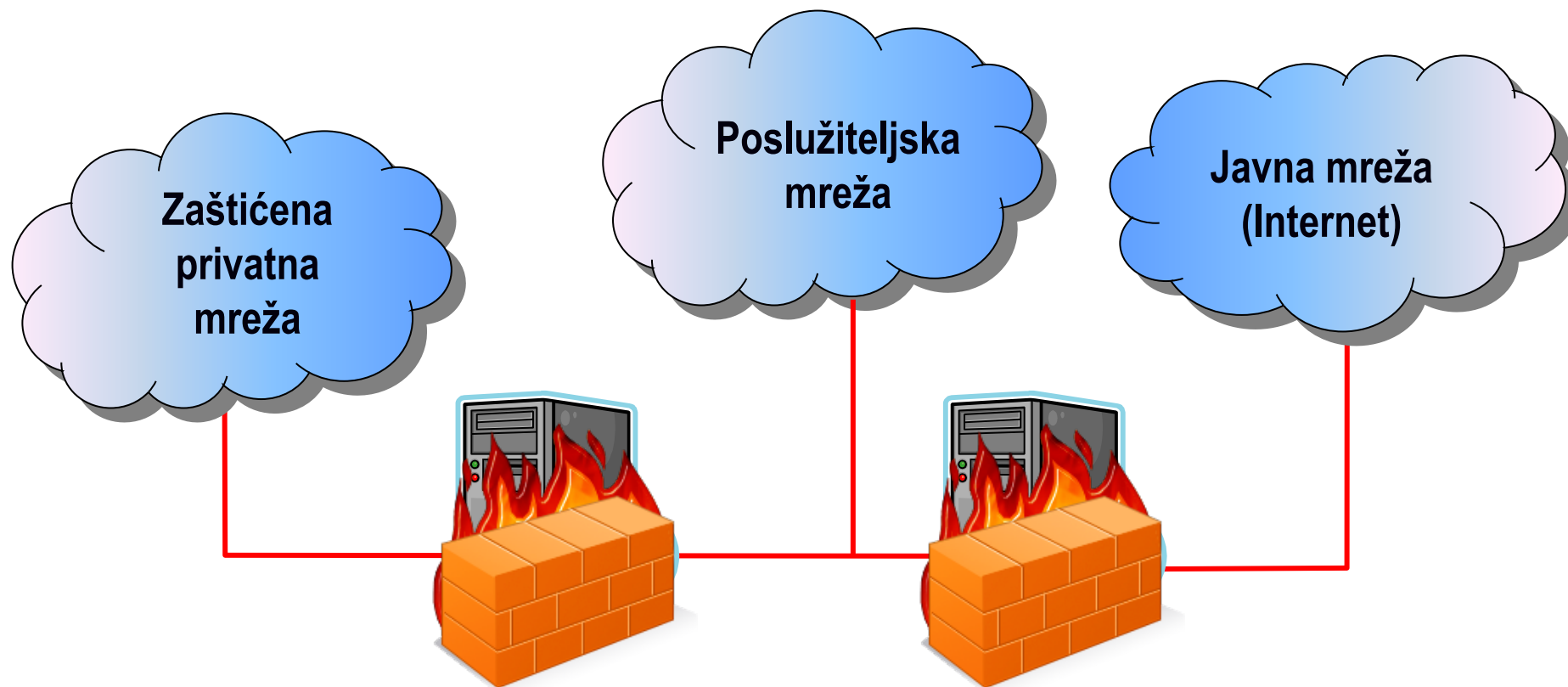


Privatne mreže s uslugama za vanjske korisnike II



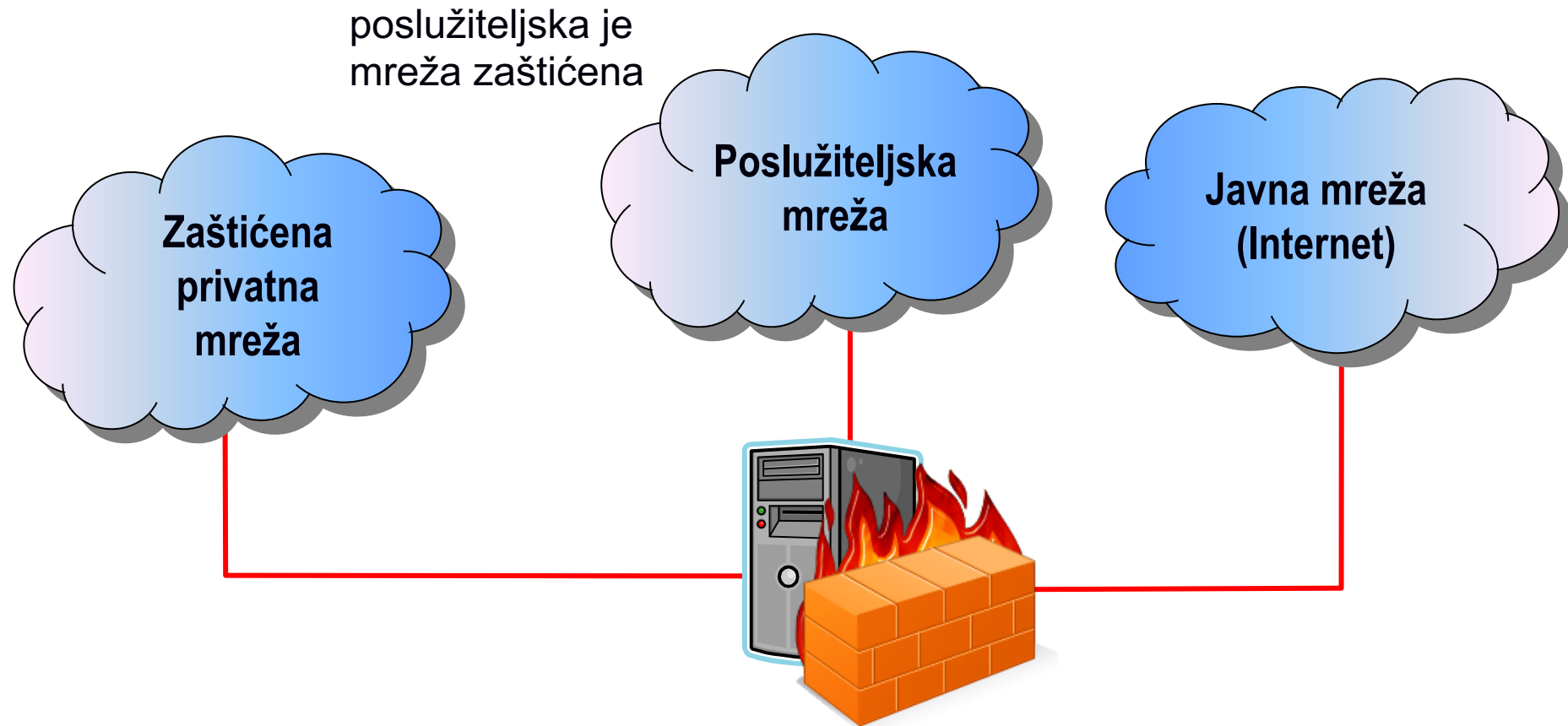
Privatne mreže s uslugama za vanjske korisnike III

- “Demilitarizirana zona”



poslužiteljska je
mreža zaštićena
dodatnim vatrozidom

Demilitarizirana zona



Filtriranje paketa – “*packet filter*”

- “packet filter” usmjerava i filtrira pakete između unutarnjih i vanjskih računala
- selektivno propušta ili blokira određene tipove paketa na temelju:
 - protokola (TCP, UDP, ICMP, ...)
 - IP adresa izvora / odredišta
 - TCP ili UDP izvorišni / odredišni port
 - TCP zastavica (SYN, ACK, FIN, ...)
 - tipa ICMP poruke
 - ...

Pravila za filtriranje

- svako pravilo specificira:
- uzorak:
 - izvorišna adresa i broj porta
 - odredišna adresa i broj porta
 - prisustvo ili odsustvo zastavica
 - akciju (dozvoli / zabrani)
- na svaki primljeni paket pravila se primjenjuju po redu
 - ako pravilo zadovoljava postavljene uvjete izvodi se odgovarajuća akcija
 - ako niti jedno pravilo ne zadovoljava, izvodi se pretpostavljena (default) akcija:
 - prihvati, propusti – Accept
 - odbaci, odbij – Reject
 - ispusti – Drop

Filtriranje paketa

- prednosti
 - jednostavna implementacija (temelji se na postojećem hardveru)
 - dobre performanse
- ograničenja
 - ograničena provjera
 - složena konfiguracija
 - nije dovoljno fleksibilno i proširivo
 - može se zaobići tuneliranjem informacija
 - može biti ranjivo na spoofing
 - fragmentirani datagrami:
 - odbacuju se kad nema dovoljno informacija za primjenu filtra
 - ako prvi frag. sadrži dovoljno informacija ostali se propuštaju bez provjere: prvi frag. s bezazlenim vrijednostima, ostali s pomakom različitim od 0 prebrišu te vrijednosti s opasnim podacima i ponovno sastavljeni fragment se dostavlja zaštićenoj usluzi!

Stateful Inspection

- radi kao paket filter (pristupne liste)
+ održavanje stanja
 - provjera i održavanje informacije o stanju svake konekcije
- dohvaća i informacije iz protokola na višim slojevima
 - moguće je pratiti slijed sesije (na primjer za FTP)
 - virtualne sesije za beskonekcijske protokole (UDP)
 - vatrozid prema podatke o portovima korištenim u određenim UDP transakcijama
 - kreiraju se privremena pravila koja propuštaju odgovor
 - provjera svakog paketa
 - ponekad se preskače provjera paketa koji je dio uspostavljene konekcije

Primjer vatrozida: netfilter / iptables (Linux)

- iptables se koristi za postavljanje, održavanje i provjeru pravila IP vatrozida ugrađenog u Linux kernel (netfilter)
<https://netfilter.org/documentation/index.html#documentation-howto>
- pravila su organizirana u lance (“chains”)
 - lanci (uređene liste) se mogu pridružiti različitim fazama obrade datagrama
stuffphilwrites.com/wp-content/uploads/2018/09/FW-IDS-iptables-Flowchart-2018-09-01.png

Primjer vatrozida: netfilter / iptables (Linux)

- „Chains”:
 - prerouting
 - input - ulazni
 - output - izlazni
 - forward - prosljeđivački
 - postrouting
 - korisnički specificirani lanci
 - dozvoljeno je „skočiti” („jump”) na drugi lanac pravila
 - može se koristiti za implementaciju translacije mrežnih adresa (NAT)
 - source translation – masquerading
 - destination translation – port forwarding

Filteri: *input / output / forward*

- lanac se sastoji od niza pravila koja se obrađuju slijedno
- ako paket zadovoljava zadani uzorak izvodi se definirana akcija, skok („jump”) na sljedeći lanac
- obrada završava ako se „skače” na lance:
 - ACCEPT – paket se prihvaća
 - DROP – paket se odbacuje
 - REJECT – kao DROP ali šalje icmp poruku ili tcp reset

Naredbe

-A, --append dodaj pravilo na kraj
lanca

```
iptables -A INPUT --dport 22 -j ACCEPT
```

-D, --delete obriši pravilo

```
iptables -D INPUT --dport 80 -j DROP
```

```
iptables -D INPUT 1
```

-I, --insert ubaci pravilo pod definiranim
rednim brojem

```
iptables -I INPUT 1 --dport 80 -j ACCEPT
```

-L, --list ispiši pravila

```
iptables -L INPUT -n -v
```

-F, --flush obriši sva pravila iz
definiranog lanca

```
iptables -F INPUT
```

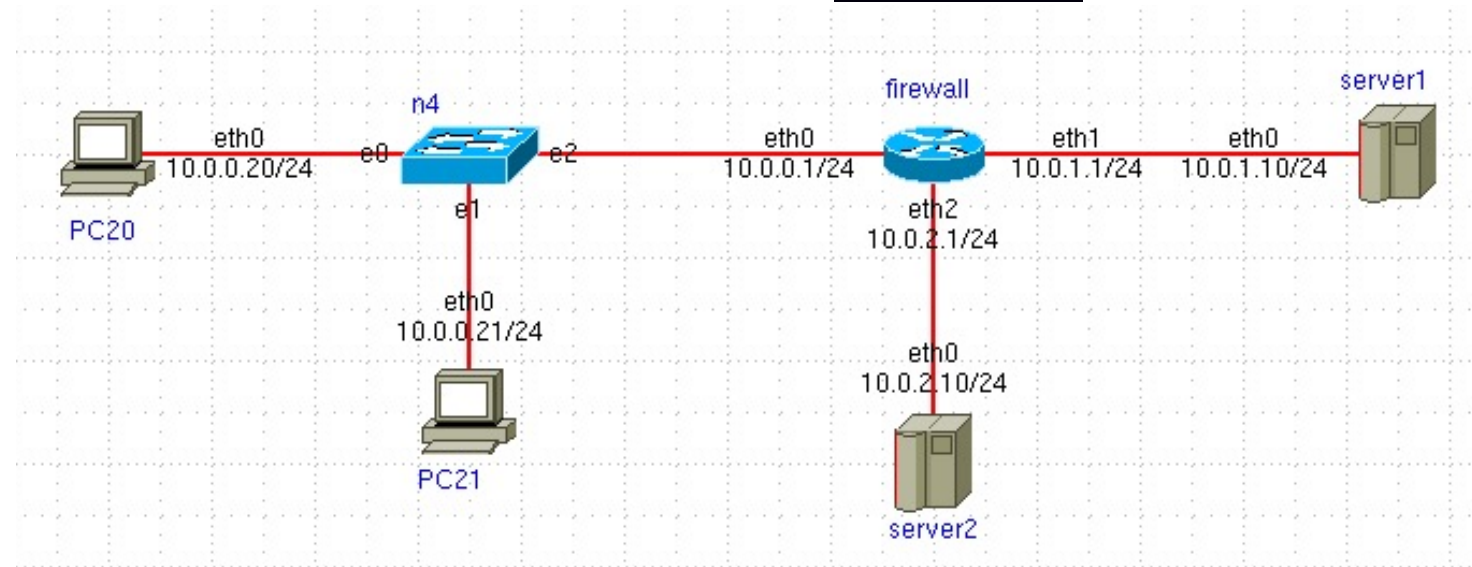
-P, --policy *defaultna* politika
(implicitno zadnje pravilo)

```
iptables -P INPUT DROP
```

Uzorci u pravilima

- generički uzorci
 - p --protocol na primjer tcp, udp, icmp
 - s --src izvorišna IP adresa
 - d --dst odredišna IP adresa, na primjer 10.1.2.3 ili 10.2.3.0/24
 - i --in-interface dolazno sučelje, na primjer eth0
 - o --out-interface odlazno sučelje
- uzorci za protokole UDP i TCP (-p udp ili -p tcp)
 - sport --source-port izvorišni port
 - dport --destination-port odredišni port
- uzorci za protokol ICMP (-p icmp)
 - icmp-type tip icmp poruke, na primjer „echo request”: --icmp-type 8
- stanje konekcije:
 - m state ESTABLISHED, RELATED
 - m conntrack --ctstate ESTABLISHED, RELATED

Primjeri korištenja



```
firewall# iptables -L -v
```

```
Chain INPUT (policy ACCEPT 0 packets, 0 bytes)
```

```
Chain FORWARD (policy ACCEPT 0 packets, 0 bytes)
```

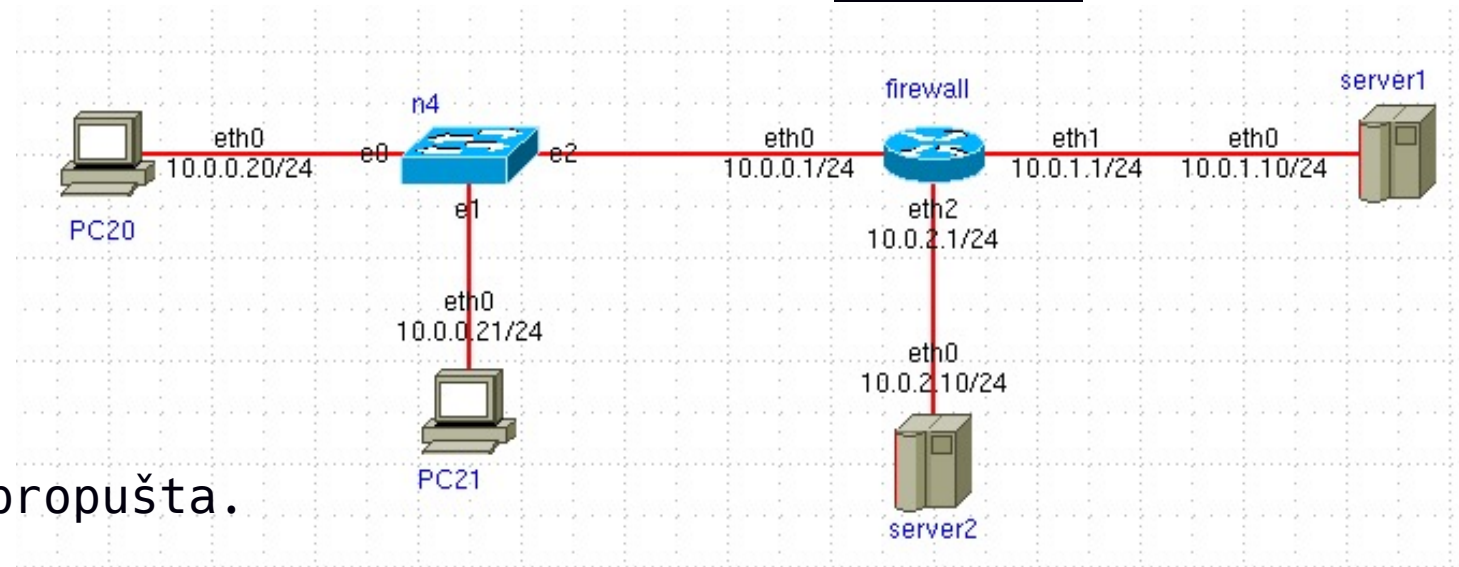
```
Chain OUTPUT (policy ACCEPT 0 packets, 0 bytes)
```

```
firewall# iptables -P INPUT DROP
```

```
firewall# iptables -P OUTPUT DROP
```

```
firewall# iptables -P FORWARD DROP
```

Primjeri korištenja



PC20# ssh 10.0.1.10

→ ne prolazi, na eth0@firewall dolazi SYN ali ga firewall ne propušta.

```
# iptables -A FORWARD -p tcp -s 10.0.0.20 -d 10.0.1.10 --dport 22 -j ACCEPT
```

PC20# ssh 10.0.1.10

→ i dalje ne prolazi, na server1 dolazi SYN, on vraća SYN+ACK ali firewall to ne propušta (paket se vidi na eth1@firewall)

```
# iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

PC20# ssh 10.0.1.10 ← prolazi jer je "established"

The authenticity of host '10.0.1.10 (10.0.1.10)' can't be established.

Primjeri korištenja

```
# iptables -A FORWARD -p icmp \
  -s 10.0.1.10 -j ACCEPT
```

```
# himage server1 ping 10.0.0.20
```

```
64 bytes from 10.0.0.20: icmp_seq=34 ttl=63 time=0.269 ms
```

→ Prolazi i odgovor jer je “established”!

```
# himage PC20 ping 10.0.1.10
```

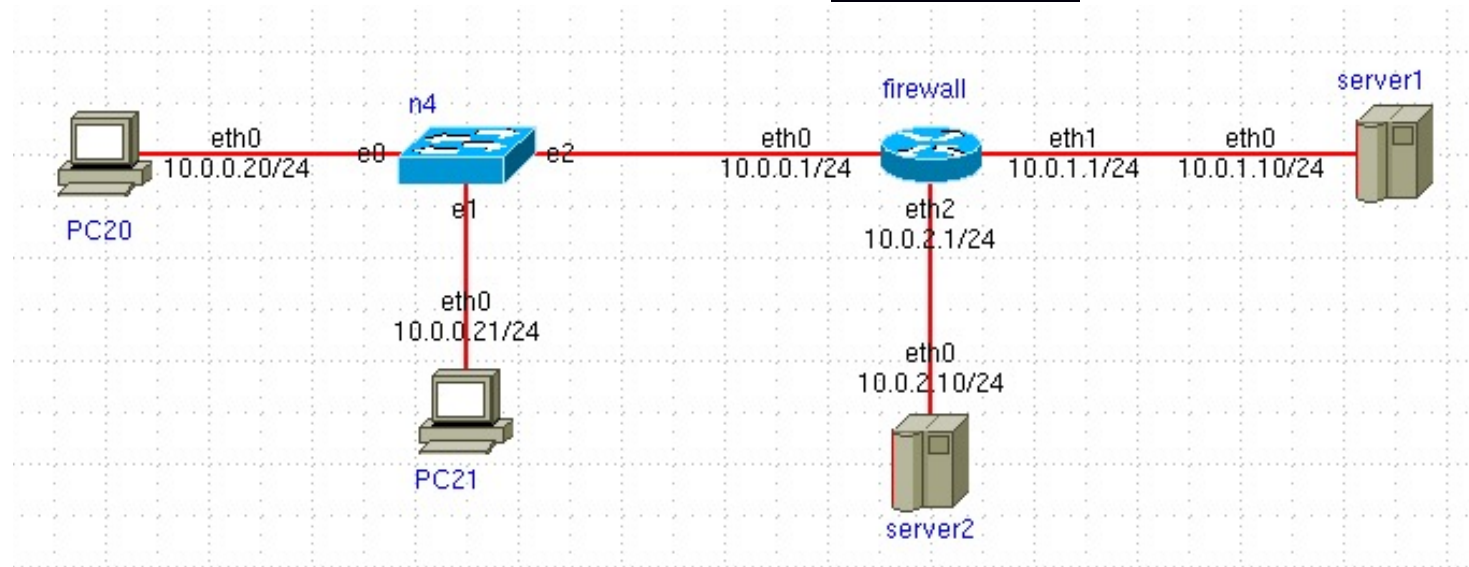
→ ne prolazi jer nije “established”!

```
# himage server2 nc -u -l -p 1234
```

```
# iptables -A FORWARD -p udp -d 10.0.2.10 --dport 1234 -j ACCEPT
```

```
# himage PC20 nc -u 10.0.2.10 1234
```

→ prolazi (“established”!)



iptables – jednostavan primjer

```
#!/bin/sh
cmd="/sbin/iptables"

$cmd -P INPUT DROP          # default policy
$cmd -P OUTPUT DROP
$cmd -P FORWARD DROP

$cmd -F INPUT                # obriše sva pravila
$cmd -F OUTPUT
$cmd -F FORWARD

$cmd -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$cmd -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
$cmd -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT

$cmd -A FORWARD -p tcp -s 10.0.0.20 -d 10.0.1.10 --dport 22 -j ACCEPT
$cmd -A FORWARD -p tcp -s 10.0.0.21 -d 10.0.1.10 \
-m multiport --dports 21,22,23,25 -j ACCEPT
$cmd -A FORWARD -p icmp -s 10.0.1.10 -j ACCEPT

$cmd -A INPUT -p tcp -s 10.0.0.21 --dport ssh -j ACCEPT
```

Primjer – Firewall Builder

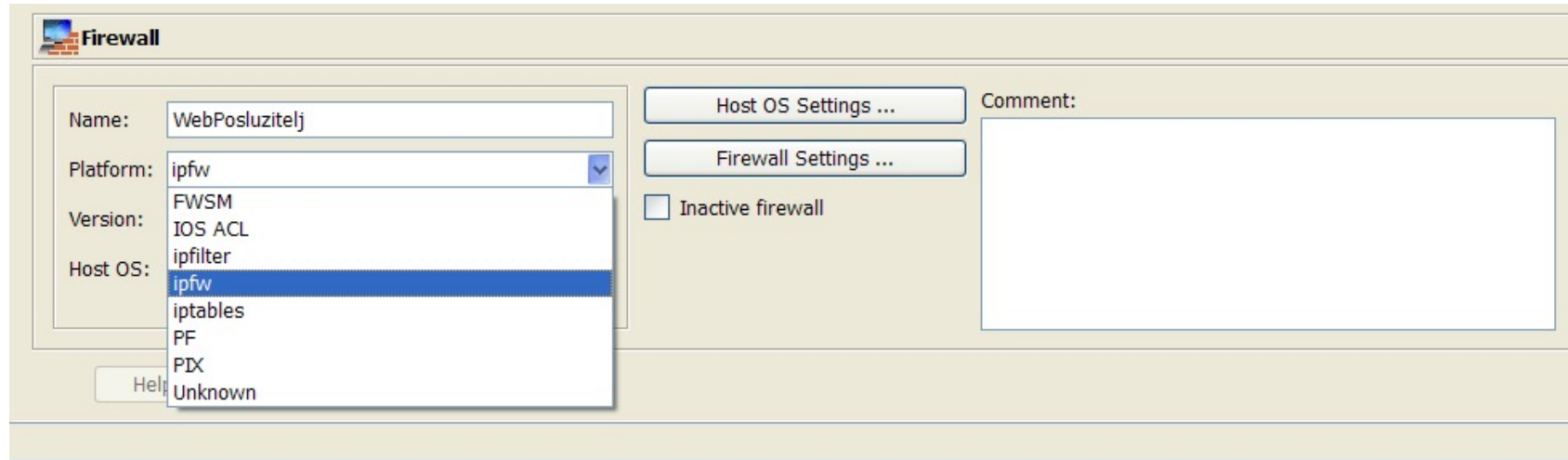
The screenshot shows the Firewall Builder application window titled "Firewall Builder - [WebPosluzitelj.fwb]". The interface includes a menu bar (File, Edit, Object, Rules, Tools, Window, Help) and a toolbar. On the left is a tree view of the project structure under the "User" tab, showing folders for Firewalls, Objects, Services, Groups, ICMP, TCP, TagServices, UDP, Users, and Time. The "WebPosluzitelj" firewall is selected, showing its configuration: outside (ext), IP WebPosluzitelj:eth0:ip, loopback, IP WebPosluzitelj:lo:ip, Policy, NAT, and Routing. Below the tree, the "Object Type" is "IPv4 address" and the "Object Name" is "WebPosluzitelj:eth0:ip" with the address "192.168.1.10/255.255.255.0".

The main area displays the "WebPosluzitelj / Policy" table with the following rules:

	Source	Destination	Service	Interface	Direction	Action	Time	Options	Comment
0	WebPosluzitelj	Any	Any	outside			Any		
1	Any	Any	Any	loopback			Any		
2	Any	WebPosluzitelj	TCP http TCP ssh Useful_ICMP	All			Any		
3	WebPosluzitelj	Any	DNS	All			Any		server needs DNS to back-resolve clients IPs.
4	WebPosluzitelj	Any	TCP smtp	All			Any		this rule allows the server to send
5	Any	WebPosluzitelj	TCP auth	All			Any		this rejects auth (ident) queries that remote
6	Any	Any	Any	All			Any		

At the bottom, the "IP Address" configuration panel is visible, showing the "Name" as "WebPosluzitelj:eth0:ip", the "Address" as "192.168.1.10", and the "Netmask" as "255.255.255.0". There is a "DNS Lookup..." button and a "Comment:" field. At the very bottom are "Help", "Apply", and "Close" buttons.

Primjer – *Firewall Builder*



```
cmd="/sbin/iptables"
```

```
$cmd -P INPUT DROP
```

```
$cmd -P OUTPUT DROP
```

```
$cmd -P FORWARD DROP
```

```
$cmd -F INPUT
```

```
$cmd -F OUTPUT
```

```
$cmd -F FORWARD
```

























```
# accept established sessions
```

```
$cmd -A INPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

























```
$cmd -A OUTPUT -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
$cmd -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

Primjer – *Firewall Builder*

WebPoslužitelj / Policy								
Source	Destination	Service	Interface	Direction	Action	Time	Options	Comment
 WebPoslužitelj	Any	Any	 outside			Any	 	
Any	Any	Any	 loopback			Any		
Any	 WebPoslužitelj	TCP http TCP ssh Useful_ICMP	All			Any		
 WebPoslužitelj	Any	DNS	All			Any		server needs DNS to back-resolve clients IPs.
 WebPoslužitelj	Any	TCP smtp	All			Any		this rule allows the server to send
Any	 WebPoslužitelj	TCP auth	All			Any		this rejects auth (ident) queries that remote
Any	Any	Any	All			Any	 	

Primjer – *Firewall Builder*

WebPoslužitelj / Policy								
Source	Destination	Service	Interface	Direction	Action	Time	Options	Comment
 WebPoslužitelj	Any	Any	 outside			Any		
Any	Any	Any	 loopback			Any		
Any	 WebPoslužitelj	TCP http TCP ssh Useful_ICMP	All			Any		
 WebPoslužitelj	Any	DNS	All			Any		server needs DNS to back-resolve clients IPs.
 WebPoslužitelj	Any	TCP smtp	All			Any		this rule allows the server to send
Any	 WebPoslužitelj	TCP auth	All			Any		this rejects auth (ident) queries that remote
Any	Any	Any	All			Any		

Rule 0 (eth0 je vanjsko sučelje)

#

```
$cmd -A INPUT -i eth0 -s 192.168.1.10 -j DROP
```

```
$cmd -A FORWARD -i eth0 -s 192.168.1.10 -j DROP
```

Primjer – *Firewall Builder*

WebPoslužitelj / Policy								
Source	Destination	Service	Interface	Direction	Action	Time	Options	Comment
WebPoslužitelj	Any	Any	outside			Any		
Any	Any	Any	loopback			Any		
Any	WebPoslužitelj	TCP http ssh Useful_ICMP	All			Any		
WebPoslužitelj	Any	DNS	All			Any		server needs DNS to back-resolve clients IPs.
WebPoslužitelj	Any	TCP smtp	All			Any		this rule allows the server to send
Any	WebPoslužitelj	TCP auth	All			Any		this rejects auth (ident) queries that remote
Any	Any	Any	All			Any		

Rule 1 (loopback sučelje)

#

```
$cmd -A INPUT -i lo -j ACCEPT
```

```
$cmd -A OUTPUT -o lo -j ACCEPT
```


Primjer – Firewall Builder

WebPosluzitelj / Policy								
Source	Destination	Service	Interface	Direction	Action	Time	Options	Comment
WebPosluzitelj	Any	Any	outside			Any		
Any	Any	Any	loopback			Any		
Any	WebPosluzitelj	TCP http TCP ssh Useful_ICMP	All			Any		
WebPosluzitelj	Any	DNS	All			Any		server needs DNS to back-resolve clients IPs.
WebPosluzitelj	Any	TCP smtp	All			Any		this rule allows the server to send
Any	WebPosluzitelj	TCP auth	All			Any		this rejects auth (ident) queries that remote
Any	Any	Any	All			Any		

```
# Rule 2 (global) (1. dio)
```

```
$cmd -A INPUT -p icmp -m icmp --icmp-type 3 \
-m state --state NEW -j ACCEPT
```

```
$cmd -A INPUT -p icmp -m icmp --icmp-type 0/0 \
-m state --state NEW -j ACCEPT
```

```
$cmd -A INPUT -p icmp -m icmp --icmp-type 11/0 \
-m state --state NEW -j ACCEPT
```


Primjer – Firewall Builder




























WebPoslužitelj / Policy								
Source	Destination	Service	Interface	Direction	Action	Time	Options	Comment
WebPoslužitelj	Any	Any	outside			Any		
Any	Any	Any	loopback			Any		
Any	WebPoslužitelj	TCP http TCP ssh Useful_ICMP	All			Any		
WebPoslužitelj	Any	DNS	All			Any		server needs DNS to back-resolve clients IPs.
WebPoslužitelj	Any	TCP smtp	All			Any		this rule allows the server to send
Any	WebPoslužitelj	TCP auth	All			Any		this rejects auth (ident) queries that remote
Any	Any	Any	All			Any		

```
# Rule 2 (global) (2. dio)
```

```
$cmd -A INPUT -p icmp -m icmp --icmp-type 11/1 \
      -m state --state NEW -j ACCEPT
```

```
$cmd -A INPUT -p tcp -m tcp -m multiport \
      --dports 80,22 -m state --state NEW -j ACCEPT
```

Primjer – *Firewall Builder*

WebPosluzitelj / Policy								
Source	Destination	Service	Interface	Direction	Action	Time	Options	Comment
 WebPosluzitelj	Any	Any	 outside			Any	 	
Any	Any	Any	 loopback			Any		
Any	 WebPosluzitelj	TCP http TCP ssh Useful_ICMP	All			Any		
 WebPosluzitelj	Any	DNS	All			Any		server needs DNS to back-resolve clients IPs.
 WebPosluzitelj	Any	TCP smtp	All			Any		this rule allows the server to send
Any	 WebPosluzitelj	TCP auth	All			Any	 	this rejects auth (ident) queries that remote
Any	Any	Any	All			Any	 	

























Rule 3 (global) - serveru treba pristup DNS-u

#

```
$cmd -A OUTPUT -p tcp -m tcp --dport 53 \
    -m state --state NEW -j ACCEPT
```

```
$cmd -A OUTPUT -p udp -m udp --dport 53 \
    -m state --state NEW -j ACCEPT
```

Primjer – *Firewall Builder*

























WebPosluzitelj / Policy								
Source	Destination	Service	Interface	Direction	Action	Time	Options	Comment
 WebPosluzitelj	Any	Any	 outside			Any		
Any	Any	Any	 loopback			Any		
Any	 WebPosluzitelj	TCP http TCP ssh Useful_ICMP	All			Any		
 WebPosluzitelj	Any	DNS	All			Any		server needs DNS to back-resolve clients IPs.
 WebPosluzitelj	Any	TCP smtp	All			Any		this rule allows the server to send
Any	 WebPosluzitelj	TCP auth	All			Any		this rejects auth (ident) queries that remote
Any	Any	Any	All			Any		

Rule 4 (global) - server šalje statistike e-mailom

#

```
$cmd -A OUTPUT -p tcp -m tcp --dport 25 \
    -m state --state NEW -j ACCEPT
```

Primjer – *Firewall Builder*




























WebPosluzitelj / Policy								
Source	Destination	Service	Interface	Direction	Action	Time	Options	Comment
 WebPosluzitelj	Any	Any	 outside			Any		
Any	Any	Any	 loopback			Any		
Any	 WebPosluzitelj	TCP http TCP ssh Useful_ICMP	All			Any		
 WebPosluzitelj	Any	DNS	All			Any		server needs DNS to back-resolve clients IPs.
 WebPosluzitelj	Any	TCP smtp	All			Any		this rule allows the server to send
Any	 WebPosluzitelj	TCP auth	All			Any		this rejects auth (ident) queries that remote
Any	Any	Any	All			Any		

Rule 5 (global) – odbaci autentifikacijske zahtjeve (ident)

#

```
$cmd -A INPUT -p tcp -m tcp --dport 113 -j REJECT
```

Primjer – *Firewall Builder*

WebPoslužitelj / Policy								
Source	Destination	Service	Interface	Direction	Action	Time	Options	Comment
 WebPoslužitelj	Any	Any	 outside			Any	 	
Any	Any	Any	 loopback			Any		
Any	 WebPoslužitelj	TCP http TCP ssh Useful_ICMP	All			Any		
 WebPoslužitelj	Any	DNS	All			Any		server needs DNS to back-resolve clients IPs.
 WebPoslužitelj	Any	TCP smtp	All			Any		this rule allows the server to send
Any	 WebPoslužitelj	TCP auth	All			Any	 	this rejects auth (ident) queries that remote
Any	Any	Any	All			Any	 	

Rule 6 (global) - zapiši sve ostale pakete

```
$cmd -N RULE_6
```

```
$cmd -A OUTPUT -j RULE_6
```

```
$cmd -A INPUT -j RULE_6
```

```
$cmd -A RULE_6 -j LOG --log-level info \
```

```
    --log-prefix "RULE 6 -- DENY "
```

```
$cmd -A RULE_6 -j DROP
```

NAT - Network Address Translation

- RFC 3022
- pretvorba privatnih IP adresa (iz privatne mreže) u globalno jedinstvene javne IP adrese
 - više računala iz privatne mreže pristupa Internetu korištenjem jedne javne IP adrese (ili nekoliko adresa)
- NAT je u osnovi *proxy* – jedan host šalje zahtjeve u ime svih internih računala
 - implementiran na transportnom sloju
- informacije skrivene u podacima (na višim slojevima) se ne mijenjaju – moguće iskorištavanje slabosti sustava
- načini rada:
 - statička translacija
 - dinamička translacija
 - translacija s balansiranjem opterećenja
 - “*network redundancy translation*”

NAT

- statička translacija
 - koristi se kad postojeći resursi unutar privatne mreže moraju biti javno dostupni
 - preslikava područje javnih IP adresa u blok iste veličine s privatnim adresama
 - primjer: 161.53.19.0–161.53.19.255 → 10.1.2.0–10.1.2.255.
 - jednostavna statička translacija za svaku korištenu IP adresu
- “port forwarding”
 - tip statičke translacije u kojem se proslijeđuje promet za samo određeni port a ne za cijelu IP adresu
 - primjer: e-mail poslužitelj je na 10.1.1.21, a vanjska IP adresa na NAT uređaju je 161.53.19.200
 - statičko preslikavanje 161.53.19.200:25 na 10.1.1.21:25
 - može se uspostaviti puno različitih usluga na jednoj IP adresi
 - posluživanje se može obavljati na više računala u internoj mreži

NAT

- dinamička translacija
 - naziva se još “overloading”, NAPT (Network Address and Port Translation) i “single address NAT”
 - veća grupa internih klijenata dijeli jednu IP adresu (ili malu grupu internih IP adresa) u svrhu skrivanja identiteta ili proširivanja prostora raspoloživih mrežnih adresa
 - portovi na jednoj javnoj IP adresi mogu se prosljeđivati na specificirane privatne IP adrese
 - translacija se kreira tek kad unutarnji klijent uspostavlja konekciju kroz NAT
 - vanjska računala ne mogu nikako adresirati unutarnja računala koja su “zaštićena” korištenjem dinamički transliranih IP adresa.
 - tehnički je moguće koristiti IP “source-routing” za usmjeravanje kroz NAT ali svi NAT uređaji takve pakete odbacuju!

NAT

- balansiranje opterećenja
 - balansiranje opterećenja poslužitelja korištenjem statičkog NAT
 - slično dinamičkoj translaciji ali u drugom smjeru
 - FW odabire kojem od poslužitelja (iz poola) treba proslijediti zahtjev
 - radi sa stateless protokolima ili protokolima koji održavaju stanje na klijentu
- mrežna redundancija
 - balansiranje opterećenja linkova prema ISP
 - automatsko prebacivanje na drugi link
 - radi s dinamičkom translacijom na isti način kao što balansiranje opterećenja radi sa statičkom translacijom
 - FW povezan na više ISP-ova
 - svako (vanjsko) sučelje ima javnu adresu
 - interna adresa je jedinstvena
 - za svaku konekciju određuje preko koje mreže treba ostvariti vezu
 - na temelju opterećenja linkova
 - linkovi koji ne rade tretiraju se kao potpuno opterećeni linkovi

Problemi s NAT-om

- neki protokoli ne rade ispravno kad se promijeni broj porta
- nekoliko protokola ne može se koristiti uz (standardni) NAT jer:
 - zahtijevaju otvaranje povratnog kanala prema klijentu (H.323 video telekonferencije)
 - informacije o TCP/IP adresi sadržane su u protokolima na višim slojevima (FTP)
 - TCP zaglavlje je šifrirano (PPTP i IPSec AH - fw mora biti krajnja točka)
 - koriste originalne IP adrese iz razloga sigurnosti
- napredniji FW može analizirati odlazne konekcije tih protokola i uspostaviti translacije koje će čekati odgovor
 - ili se koriste specifični posrednički programi (*proxy*) u kombinaciji s NAT mehanizmima
- teoretski najviše 65,536 konekcija na jednoj IP adresi
 - u pravilu ograničeno na < 50,000 konekcija (portovi rezervirani za druge namjene)
 - na Linuxu standardno omogućeno korištenje 4096 portova

Sigurnost?

- NAT skriva klijente te ih nije moguće hakirati. → Ne! Moguće je!
 - statička translacija ne štiti unutarnja računala
 - zamjenjuje informacije o portovima jedan-na-jedan te se i napadi translatiraju kao i regularni zahtjevi
 - ako klijent uspostavi konekciju postoji i povratna veza
 - ako se konekcija može presretati ili je podložna napadu “*man-in-the-middle*” tada je “*man-in-the-middle*” krajnja točka.
 - loša implementacija omogućava “provalu” na NAT
 - *Source routing*
 - upiše se cijeli puta do odredišta
 - NAT uređaj se upiše kao jedna od adresa
 - NAT usmjerava datagram do krajnjeg odredišta
 - FW/NAT obavezno mora odbacivati takve datagrame

Sigurnost?

- prijevara s internog računala
 - korisnik iz neznanja ili nepažnje pročita falsificirani e-mail s linkom na web stranicu ili posjeti “opasne web stranice” te učitava softver koji skriva Trojanskog konja
 - rješenje je u primjeni aplikacijski specifičnih posrednika
 - rade na visokom sloju
 - provjeravaju sadržaj koji protokol razmjenjuje (na primjer u HTTP protokolu traže sumnjive sadržaje: Java applet, ActiveX kontrole, izvršni programi, ...)
- problem vremenskih kontrola tablice stanja
 - FW se ne može pouzdati na informacije o zatvaranju sesije
 - mnogi protokoli nemaju očigledan završetak
 - vremenske kontrole mogu znatno varirati i u pravilu nisu objavljene
 - prije isteka vremenske kontrole postojeća konekcija se može zloupotrijebiti
 - uz poznavanje točne IP adrese i porta te originalne IP adrese

Sustavi za detekciju upada (1)

- engl. Intrusion Detection Systems
- Temelje se na ideji da se praćenjem ponašanja sustava ili prometa na mreži može detektirati incident
- Podjele prema načinu rada
 - Bazirane na pravilima
 - Na detekciji ponašanja ili anomalijama
- Podjele prema mjestu nadzora
 - Mrežni (NIDS) – uzimaju podatke s mreže
 - Računalni sustavi (HIDS) – uzimaju podatke s računala

Sustavi za detekciju upada (2)

- Mrežni sustavi
 - Postavljaju se na neke ključne točke na kojima snimaju promet
 - Bitno je da vide promet mrežnog segmenta kojeg želimo pratiti
 - Mogući problemi s brzinama (10G+)
 - Problem je i šifrirana komunikacija
- Mnoštvo različitih sustava na tržištu
 - Popularna implementacija otvorenog koda - SNORT, BRO, OSSEC, Suricata

Sustavi za prevenciju upada

- Osim detekcije rade i prevenciju
 - Intrusion Prevention Systems (IPS)
- Prevencija može biti postavljanje dodatnih pravila na vatrozidu
 - Pravila privremena ili stalna
- Ako nisu dobro podešeni mogu onemogućiti ispravan rad mreže!

Otkrivanje ranjivosti u mreži

- Ranjivosti u računalnoj mreži su neizbježne(!)
 - Treba ih što prije otkriti i ukloniti
- Otkrivanje ranjivosti može se obaviti na dva temelja načina
 - Skeniranje mrežnih raspona
 - Nessus, OpenVAS
 - Jednostavno, ali opterećuje mrežu i puno lažno točnih detekcija
 - Jeftina, ali ne otkrivaju nužno sve ranjivosti
 - Penetracijska ispitivanja
 - Obavljaju pojedinci ili timovi koji traže ranjivosti
 - Cilj je i pokušati iskoristiti ranjivost, ne samo ju naći
 - Skuplja od skeniranja
 - Ne otkrivaju nužno sve ranjivosti

Honeypot

- mamac (engl. honeypot) je nekakvo računalo ili računalni resurs čija isključiva namjena je da bude iskorišten ili manipuliran na nekakav način
 - mamac može biti računalo, usluga, podatak
- ideja je na mrežu staviti računala i usluge koje nitko ne koristi i potom pratiti kada im netko pristupa
 - pristup znači nedozvoljenu aktivnost!
- podjela
 - visoke interakcije (cijelo računalo) ili niske interakcije (samo pojedina usluga, možda ne u cijelosti)