# Linux vatrozidi za vašu lokalnu mrežu

Dobrica Pavlinušić

Fakultet Organizacije i Informatike Varaždin

Hrvatska Udruga Linux Korisnika

# Sadržaj

- zašto postaviti vatrozid?
- tipovi vatrozida (koji odabrati?)
- način implementacije
- PRO/CON analiza
- instalacija Linux-a kao za vatrozida (odabir paketa, upgrade distribuciju)
- što pratiti na mreži

# TEORIJA

# Sigurnosne politike

Što pokušavamo zaštititi?

Protiv koga štitimo računarski sustav?

Koliko si sigurnosti možemo priuštiti?

Obrazovanje korisnika

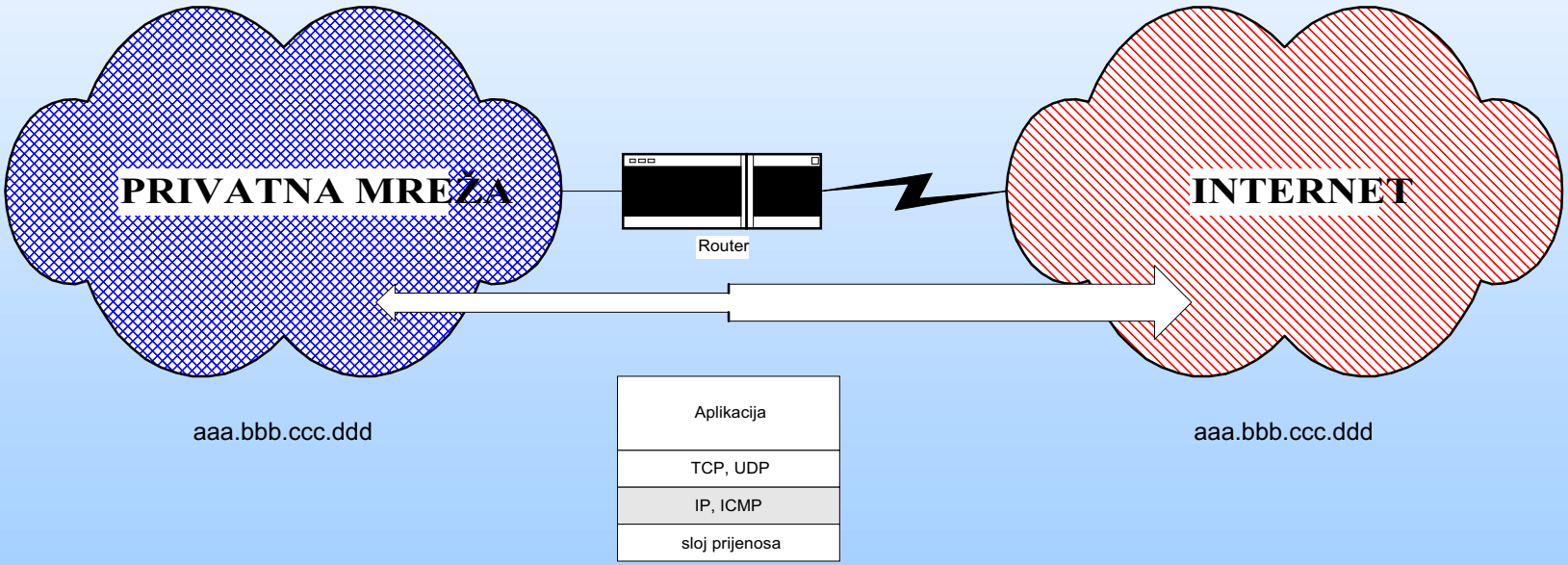
# Tipovi vatrozida

**Filtrirajući routeri**

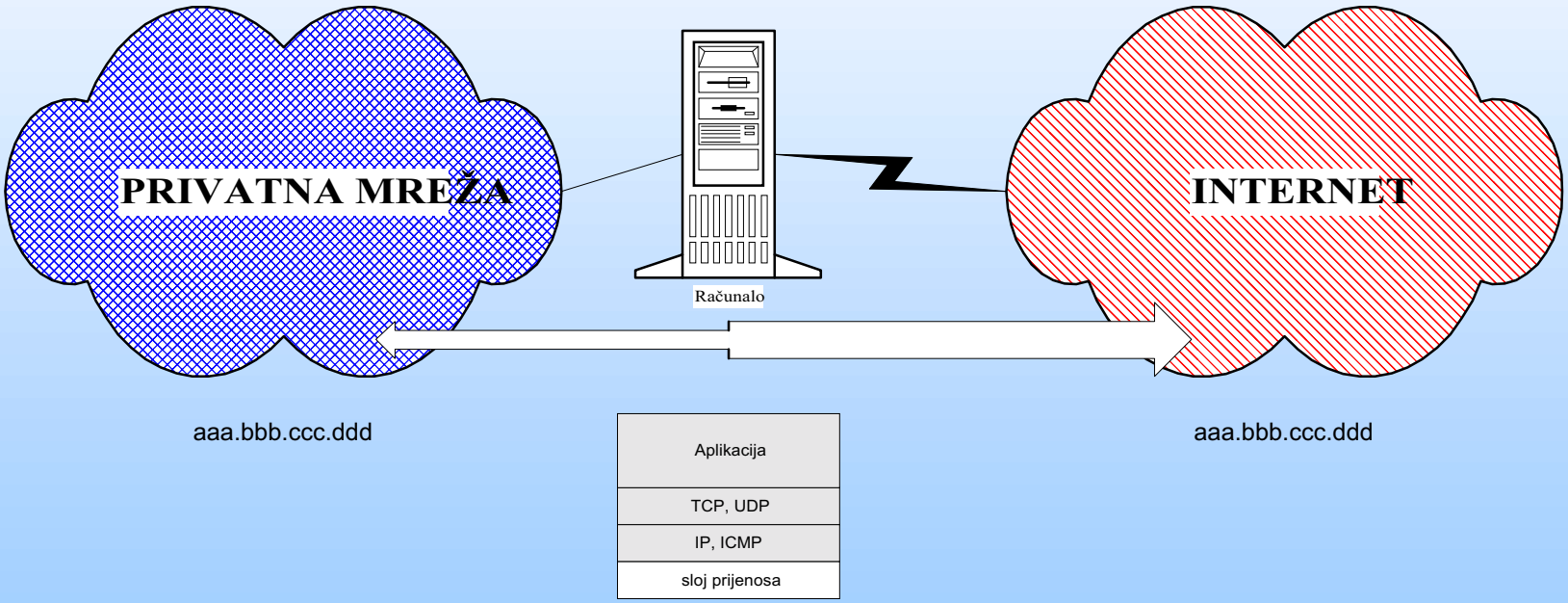
**Vatrozidi zasnovani na hostu**

**Izolacijske mreže**

# Filtrirajući routeri



# Vatrozidi zasnovani na hostu



# Izolacijske mreže


192.168.ccc.ddd

aaa.bbb.ccc.ddd
192.168.ccc.ddd

aaa.bbb.ccc.ddd

# PRO/CON analiza

- veća zaštita
- lakše administriranje
- veća praćenja aktivnosti korisnika (*logging*)
- jednostavnije dodavanje novih računala

- gubitak dijela servisa
- uznemirivanje korisnika dodatnom sigurnošću
- kompliciranо održavanje
- kod naknadnog uvođenja vatrozida rekonfiguriranje

# PRAKSA

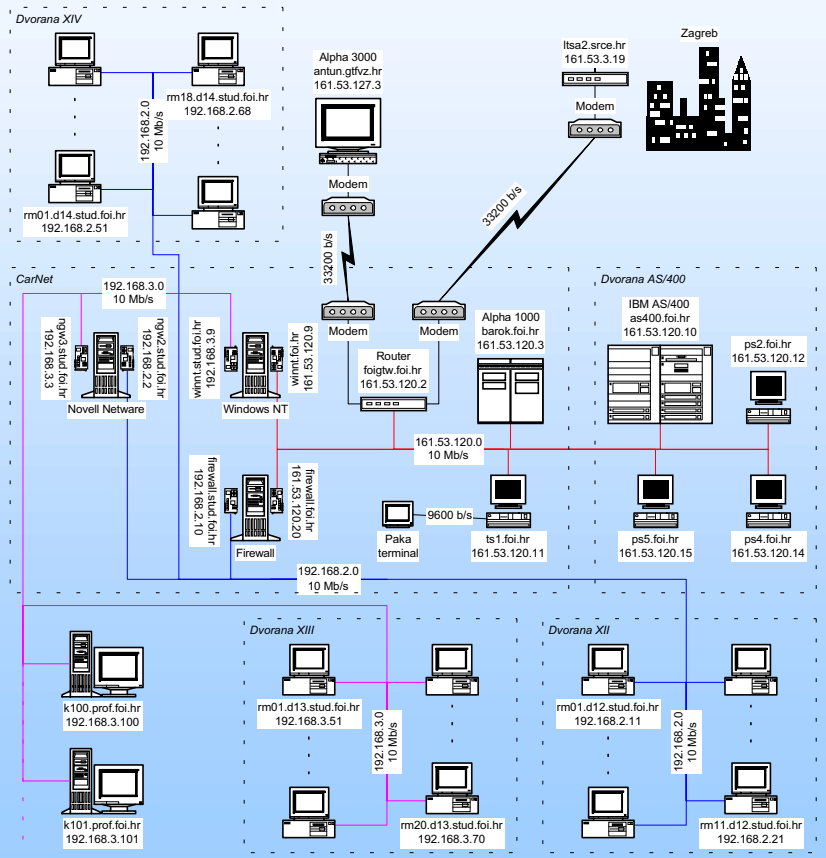
# Instalacija Lunux-a

**koju distribuciju odabrati**

**odabir paketa za instalaciju**

**da li raditi upgrade**

# Naša lokalna mreža



# Koji tip vatrozida?

- Zasnovan na host-u, sa izolacijskom mrežom
  - proxy (squid)
    - www, gopher, ftp
  - anonymous ftp server
  - news server (nntpcache)
  - ostali proxy servisi
    - realaudio, socks, baze podataka, ...

# Način implemetacije

- Evolucijski model sa mnogim primjenama principa pokušaja i pogreške
- Osiguravanje opreme
  - računalo
  - mrežne kartice
  - diskovi
- Redundantne komponente

# Što instalirati

- Osnovno, pa ručno dodavati pakete
  - slackware (A, AP, N)
- Uobičajno pa ukloniti nepotrebne pakete
  - RadHat
- Kombinacija
  - neizbježna, najteža za održavanje
- Da li raditi upgrade?

# ISKUSTVA

- Zadovoljstvo sigurnošću mreže i mogućnošću praćenja korisnika
- Korisnici zadovoljni ponudom servisa
- Jednostavnost administriranja računala na lokalnoj mreži
- Prevelika ovisnost o vatrozidnom računalu

# Što pratiti na mreži:

News grupe

- hr.comp.security
- comp.security.announce - objave CERT-ovih upozorenja o sigurnosnim problemima
- comp.security.unix - rasprave o sigurnosti pod Unix-om
- comp.security.* - rasprave o ostalim temama vezanim za sigurnost (pgp, ssh, ...)

# Što pratiti na mreži:

## Mail liste

- linux-alert@redhat.com
  - moderirana lista za obavjesti (diskusije se nalaze na linux-security@redhat.com) <URL: http://www.redhat.com/linux-info/security/linux-alert/>
- BUGTRAQ@netspace.org
  - lista poznatih sigurnosnih propusta, arhiva se nalazi na <URL: http://www.geek-girl.com/bugtraq/archives.html>

# Što pratiti na mreži:

## WWW adrese

- <URL: http://www.aoy.com/Linux/Security/Linux-Security-FAQ/> Linux Security Alerts, dodatak FAQ-u o sigurnosti linux-a
- <URL: http://www.rootshell.com/> Kolekcija od više od 500 poznatih načina za provaljivanje u računarske sustave
- <URL: http://www.efri.hr/~crv/security/> Veoma dobara stranica o sigurnosti u Hrvatskoj

# ZAKLJUČAK