Linux jako router, firewall, DHCP server, proxy a DNS cache

Lukáš Zapletal, 2007-02-28
lukas.zapletal@liberix.cz

Volba distribuce

- volíme serverovou distribuci
- chceme nebo nechceme platit za služby
- nezpoplatněné distribuce:
  Ubuntu Server, CentOS, Debian
- zpoplatněné distribuce:
  RHEL, SLES, Mandriva Corporate Server
- nebo cokoli jiného poslouží stejně dobře

TCP/IP

- základní pojmy: TCP, UDP, packet, socket, IP adresa, port
- MAC adresa, ARP tabulka
- obsah packetu: zdrojová adresa, cílová adresa, zdrojový a cílový port
- síť, maska sítě, routovací tabulka
- NAT (DNAT, SNAT)

IP adresa a maska

- typické nastavení - DHCP nebo staticky (neboli ruční nastavení)
- ruční nastavení - u každé distribuce jiné
- můžete to také udělat pomocí základních nástrojů (ifconfig, route, resonv.conf)
- ifconfig - zobrazuje informace o IP adresách, MAC adresách atd
- ifconfig eth0 up 192.168.1.1 netmask XXX

MAC adresa / ARP tabulka

- příkaz arp - vypíše ARP tabulku
- v tabulce vidíme jen MAC adresy, se kterými daný stroj již komunikoval
- arping IP_ADRESA - ping přes MAC

Routování na stanici

- příkaz route (route -n)
- přidání cesty do sítě přes zařízení:
  route add -net 192.16.190.0 netmask \
  255.255.255.0 dev eth0
- route add default gw gw.firma.cz
- smazání: route del ...

Routování mezi sítěmi

- router - počítač s více síťovými rozhraními (nebo jedným + switch + virtuální IP)
- postup je stejný - nastavení příkazem route
- klient 1 - síť A - router - síť B - klient 2
- router přijímá packety na eth0 například a posílá je na eth1 (do jiné sítě)
- je nutno zapnout routování mezi rozhr.: echo "1" > /proc/sys/net/ipv4/ip_forward
- další pojmy: metriky, RP filtry (falšování)

DNS

- služba pro překlad z jmen na IP adresy a opačně
- získá se z DHCP
- /etc/resolv.conf

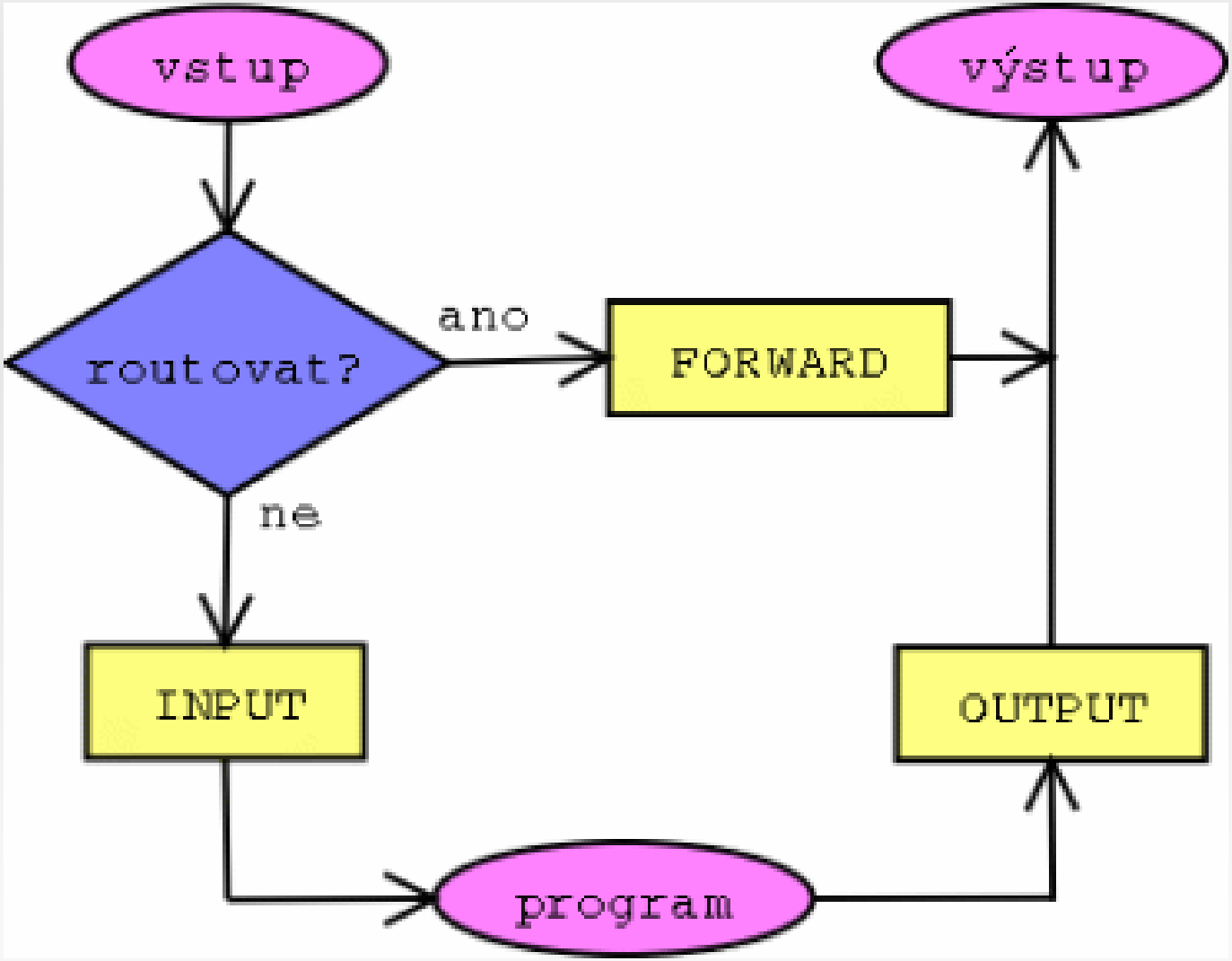
Firewall

- linuxové jádro má v sobě zabudován velmi mocný firewall s podporou NATu (překlad adres - „schování“ celé sítě pod jednu IP adresu (SNAT) / „přesměřování“ příchozího provozu z internetu (DNAT))
- ve většině distribucí (všech serverových) je tato podpora zakompilována (obvykle jako moduly)
- tyto moduly je nutno nahrát (při startu): modprobe ipt_LOG ipt_REJECT ipt_MASQUERADE ip_conntrack_ftp ...

Firewall

- Firewall je zařízení (zpravidla počítač) sídlící mezi sítěmi (nebo na pracovní stanici), který omezuje, monitoruje či dokonce upravuje veškeré informace proudící mezi nimi, a to oběma směry.

Firewall



Firewall

- v jádrech řady 2.4 a 2.6 se pro nastavování firewallu používá program iptables
- při startu tedy stačí zavést potřebné moduly a provést několik příkazů
- obvyklý postup: vše se na začátku zakáže a postupně se povoluje
- výborný skript (do začátku) mpfw http://www.petricek.cz/mpfw/

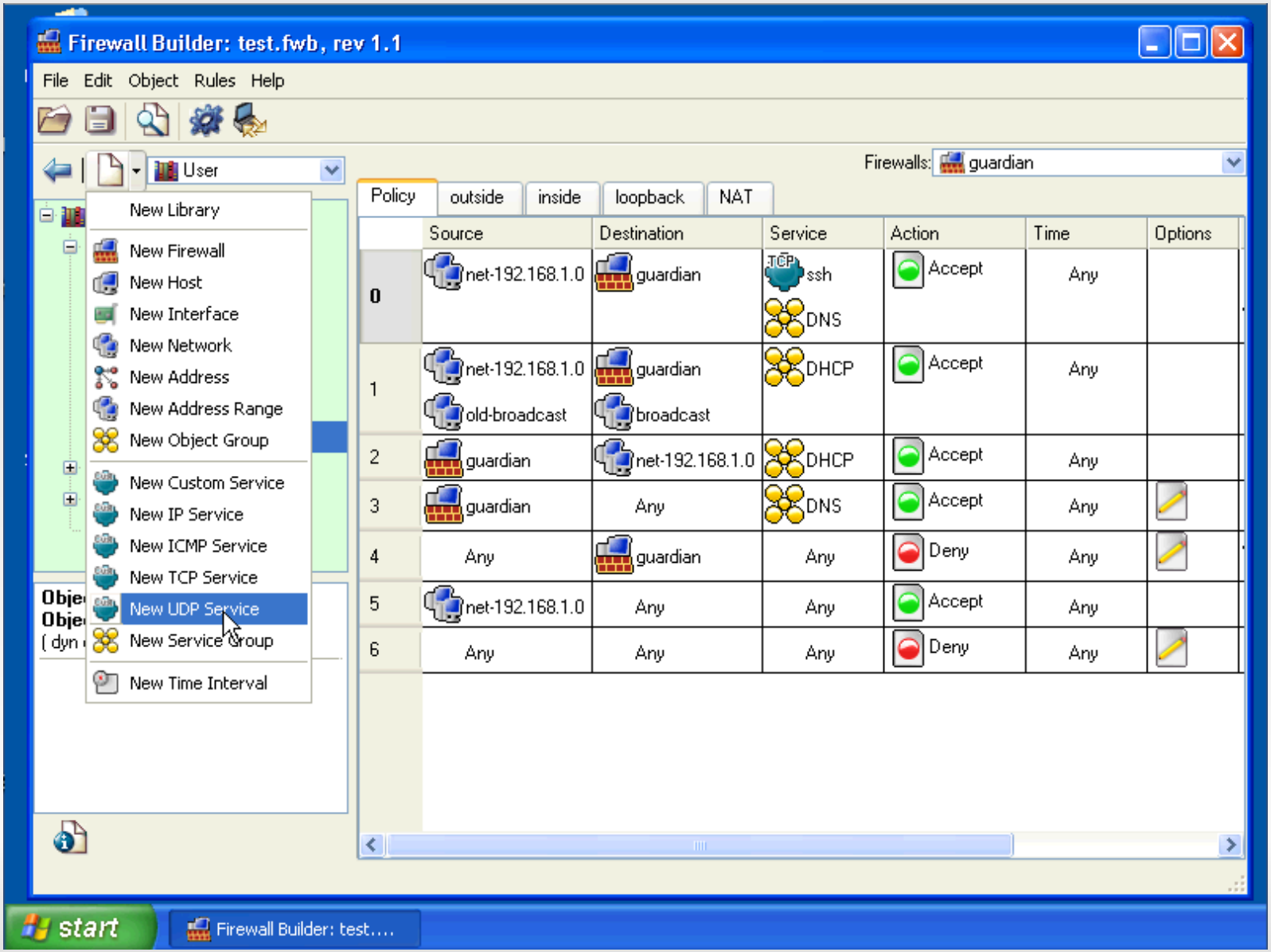
Firewall

(ukázka mpfw skriptu)

Firewall

- existují různé skripty a programy, které usnadňují (nebo zcela odstíní) „ruční“ tvorbu pravidel
- známé jsou např. Shorewall (textový) nebo FwBuilder

Firewall - FwBuilder



Proxy servery

- typickou službou, která běží u routerů/firewallů jsou proxy
- nejvíc se používá HTTP proxy
- umožňuje kontrolovat a monitorovat obsah (například omezovat zaměstnance v používání internetu v určitých hodinách, odstraňovat reklamu, logovat přístupy)
- transparentní proxy - nepotřebuje

Proxy servery

- existují proxy servery i na další služby (FTP, telnet) nebo univerzální (SOCKS)
- pokud máte proxy server, nemusíte konfigurovat NAT
- používá se obvykle v kombinaci
- nejznámější http proxy: Squid