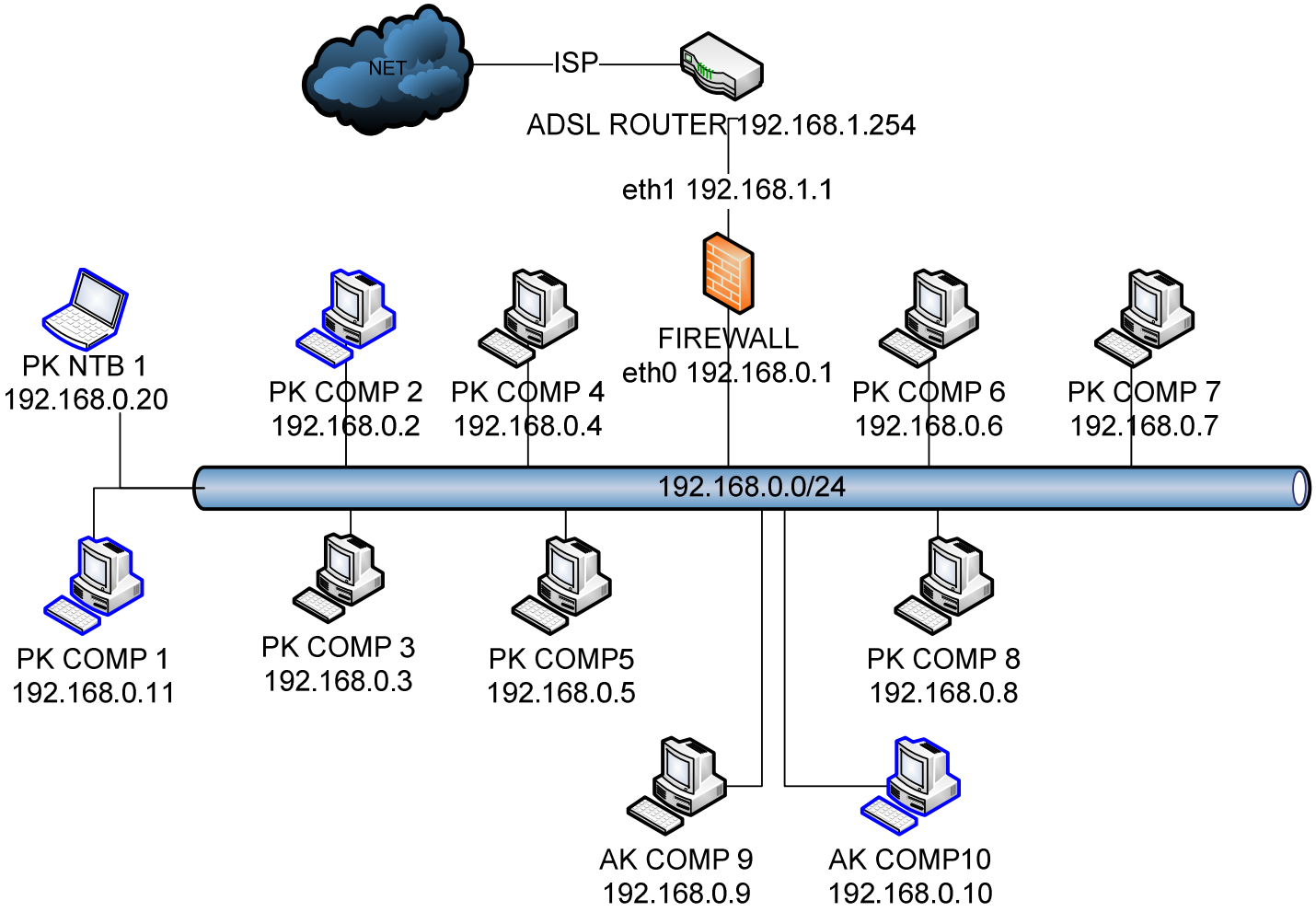
Firewall pro malou firmu

Josef Vítek

Y36SPS

Topologie sítě



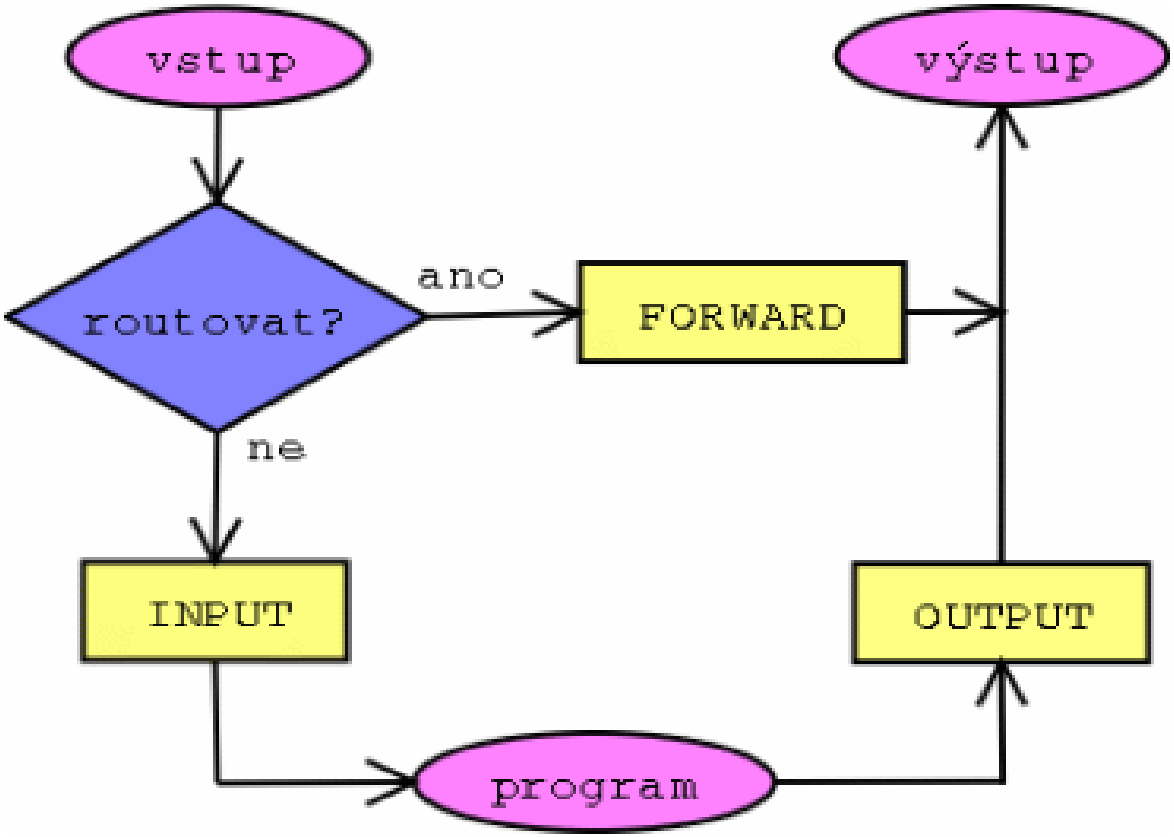
Bezpečnostní politika

- Defaultně všechno zahazovat
- Použit NAT
- Stavový firewall – příchozí pakety povoleny jenom na navázaná spojení
- Odchozí pakety jen na vybrané služby (www, ftp, pop3, imap, smtp, dns, ssl, https, rsync) + výjimky

Bezpečnostní politika

- Ochrana před spoofingem – rp_filter
- Ochrana před SYN útokem – 5 SYN paketů za sekundu
- Ochrana před skenováním portů – 10 paketů se SYN,FIN SYN,FIN flagy

Iptables - NAT



Zdroj: http://www.root.cz/clanky/stavime-firewall-1/

Iptables - NAT

IP Maškaráda

iptables -t nat -A POSTROUTING -o eth1 -j SNAT --to 192.168.1.1

Stavový firewall

iptables -A FORWARD -i eth1 -o eth0 -m state --state ESTABLISHED,RELATED -j ACCEPT

Nastavení řetězce FORWARD

iptables -A FORWARD -i eth0 -p TCP --dport 80 -j ACCEPT #WWW

...

iptables -A FORWARD -i eth0 -s 192.168.0.2 -j ACCEPT

Testování – hping3

```
hping -I eth0  -S 192.168.10.1 -p 80

HPING 192.168.10.1 (eth0 192.168.10.1): S set, 40 headers
   + 0 data bytes
len=46 ip=192.168.10.1 flags=SA DF seq=0 ttl=64 id=11101
   win=16080 rtt=2.7 ms
len=46 ip=192.168.10.1 flags=SA DF seq=1 ttl=64 id=11102
   win=16080 rtt=2.4 ms
len=46 ip=192.168.10.1 flags=SA DF seq=2 ttl=64 id=11103
   win=16080 rtt=2.4 ms
```

SA = SYN/ACK → port je otevřen

RA = RST/ACK → port není otevřen

Testování – hping3

Scanování tcp portů firewallu (služby z /etc/services):

```
hping3 --scan known 192.168.1.1
```

Scanování portů (0-65535):

```
hping3 --scan all 192.168.1.1
```

SYN útok na firewall s podvrženou lokální adresou (192.168.1.99):

```
hping3 -a 192.168.1.99 -S 192.168.1.1 -p 80 -i u1000
```

Zdroje

- http://www.root.cz/serialy/stavime_firewall/
- http://www.petricek.cz/mpfw/
- http://www.thesprawl.org/infocalypse/index.php?title=Hping
- http://www.radarhack.com/dir/papers/hping2_v1.5.pdf