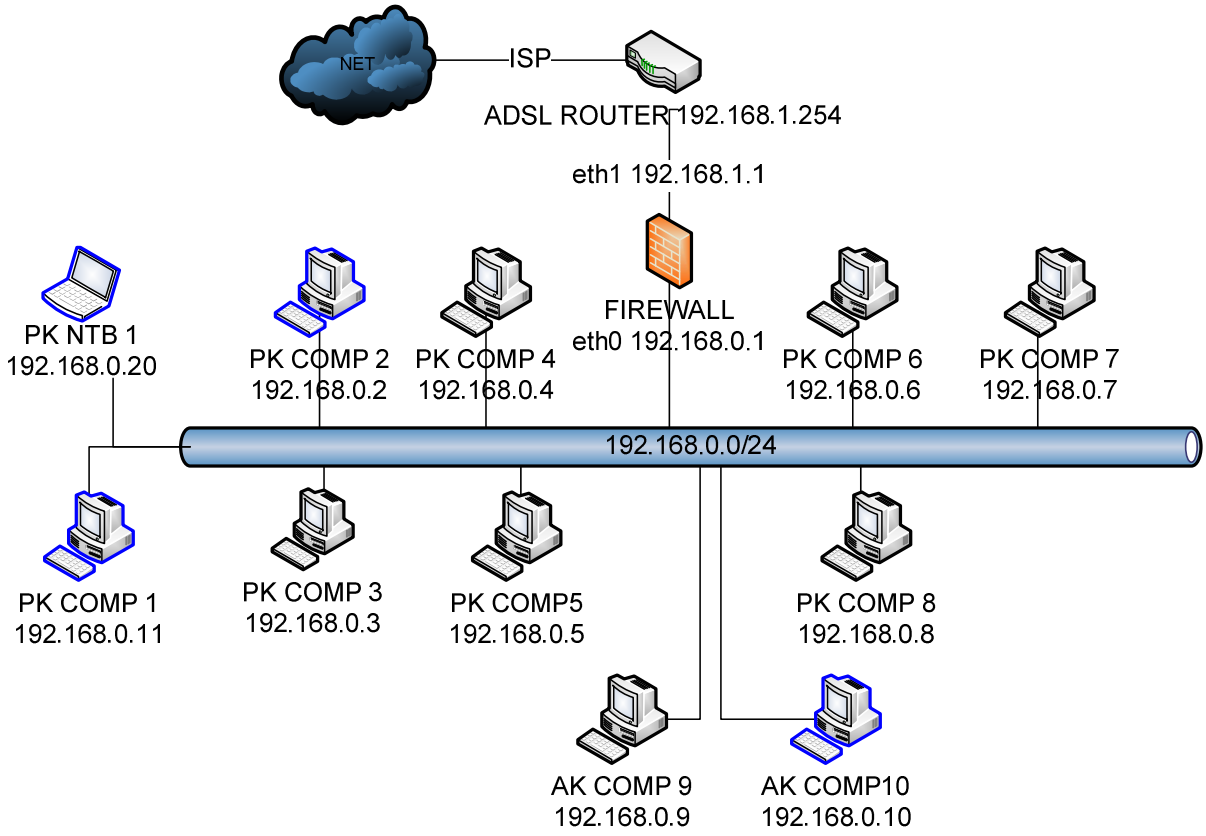
Y36SPS – Správa počítačových sítí

Josef Vítek

Firewall pro malou firmu

Topologie sítě



PK – projekční kancelář, AK – advokátní kancelář

Použité technologie

Systém: Ubuntu 8.10 Hardy Heron

Firewall: iptables

Testování firewallu: hping3

Bezpečnostní politika

Výchozí politika je zahazovat pakety na všech řetězcích (INPUT,OUTPUT,FORWARD) .

Celá síť je za ADSL modemem/routerem, na kterém běží NAT do vnitřní sítě (používá se jedna vnější IP adresa pro celou síť, není forwardována žádná další IP adresa). Z vnější sítě by se nikdo dovnitř dostat neměl, ani na webové rozhraní routeru (to je zakázáno pro vnější síť).

Firewall navíc odstiňuje uživatelské stanice od routeru. Na firewallu běží také NAT:

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

Pakety odcházející přes rozhraní eth1 (směrem k ADSL routeru) jsou maskovány adresou firewallu 192.168.1.1 .

Příchozí pakety jsou povoleny pouze takové, které se týkají již navázaného spojení, či s ním nějak souvisí.

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

Všechny počítače mají povoleno navazovat spojení ven pouze na určené služby:

- FTP
- Ssh
- SMTP
- DNS
- WWW
- POP3
- IMAP
- HTTPS
- rsync

Existují výjimky, které můžou vše (PK COMP1, PKCOMP2, PK NTB1, AK COMP 10).

```
iptables -A FORWARD -i eth0 -p TCP --dport 21 -j ACCEPT  #FTP
iptables -A FORWARD -i eth0 -p TCP --dport 22 -j ACCEPT  #SSH
iptables -A FORWARD -i eth0 -p TCP --dport 25 -j ACCEPT  #SMTP
iptables -A FORWARD -i eth0 -p UDP --dport 53 -j ACCEPT  #DNS  UDP
iptables -A FORWARD -i eth0 -p TCP --dport 53 -j ACCEPT  #DNS  TCP
iptables -A FORWARD -i eth0 -p TCP --dport 80 -j ACCEPT  #WWW
iptables -A FORWARD -i eth0 -p TCP --dport 110 -j ACCEPT #POP3
iptables -A FORWARD -i eth0 -p TCP --dport 143 -j ACCEPT #IMAP
iptables -A FORWARD -i eth0 -p TCP --dport 443 -j ACCEPT #HTTPS
iptables -A FORWARD -i eth0 -p TCP --dport 873 -j ACCEPT #rsync
```

```
iptables -A FORWARD -i eth0 -s 192.168.0.2 -j ACCEPT
iptables -A FORWARD -i eth0 -s 192.168.0.10 -j ACCEPT
iptables -A FORWARD -i eth0 -s 192.168.0.11 -j ACCEPT
iptables -A FORWARD -i eth0 -s 192.168.0.20 -j ACCEPT
```

Ochrana před spoofingem je realizována aplikací rp_filtru na ethernetová rozhraní firewallu. Dále je kontrolováno, jestli nejsou na vnějším rozhraní podvrženy pakety tvářící se jako pakety z vnitřní sítě.

Dále je aplikována ochrana před SYN floodem limitováním vstupujících SYN paketů na maximálně pět za sekundu.

Pakety skenující porty jsou také omezovány na 10 / minutu.

Testování:

Pro testování nastavení firewallu jsem použil utilitu hping3.

Scanování daného portu (80):

```
hping3 -S 192.168.1.1 -p 80
```

```
analogicky pro ostatní porty
```

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

Přílohy:

firewall.txt – skript pro spuštění firewallu