iptables LEASE target

Thomas Bader

<thomasb@trash.net>

Problemstellung

- Roadwarriors verbinden über einen Tunnel
- Sind über ihre offizielle IP im LAN sichtbar
- $\ldots \Longrightarrow$ Probleme mit Packetfilter und tcpwrapper (und andere)

Lösungsansätze

- PPPoEoI (PPP over Ethernet over IPSEC)
- Roadwarrior Adressen werden über DNAT/SNAT zu einer IP-Adresse aus dem LAN-Range gemapt

$\Longrightarrow$ zu aufwendig

Saubere Lösung

- iptables mit einem neuen Target erweitern
- Bi-Direktionales NAT
- Mappings zwischen ausgewähltem Pool und Roadwarrior Adressen
- Dazu noch Proxy ARP

$\Longrightarrow$ iptables LEASE target

Konfigurationsbeispiel

- Zuerst Pakete von Roadwarriors markieren:

```
KNOWN_RANGES="10.230.0.0/16 172.20.0.0/24"

iptables -t mangle -N lease_mark

for i in ${KNOWN_RANGES}
     iptables -t mangle -A lease_mark -s ${i} -j RETURN
done

iptables -t mangle -A lease_mark -j MARK --and-mark 0x100
iptables -t mangle -A PREROUTING -i ipsec0 -j lease_mark
```

Konfigurationsbeispiel (2)

- Mit den markierten Packeten nun das Mapping herstellen:

```
iptables -t nat -A POSTROUTING -m mark --mark 0x100/0x100 \
                -j LEASE --range 192.168.0.33-192.168.0.39
iptables -t nat -A PREROUTING -d 192.168.0.32/29 -j LEASE \
                --revmap
```

Konfigurationsbeispiel (3)

- Proxy ARP:

```
tarpd eth0 192.168.0.32 192.168.0.32 &

ip route add 192.168.0.32/29 dev ipsec0
```

Links

- http://www.trash.net/~kaber/lease/
- http://www.cs.hut.fi/~tricky/utils/net/

```
$Id: iptables-lease.slides.tex,v 1.2 2002/07/17 20:08:04 thomasb Exp $
```