NAT-Umgehung über UDP

Ingo Blechschmidt
<iblech@web.de>

LUGA

8. Juni 2005

Inhalt

Problem

- Wunsch: Bidirektionale Verbindung zwischen zwei sich hinter NAT-Gateways befindlichen Computern
- Problem: Regelwerk der Firewalls:
  „Erlaube nur Verbindungen von außen, wenn sie von innen initiiert wurden.“
- Aber wie eine Verbindung aufbauen, ohne öffentliche IP?

Lösung

- Versendung von UDP-Paketen von A an den NAT-Gateway von B
- Blocken dieser Pakete durch die Firewall von B (klar)
- Versendung von UDP-Paketen von B an den NAT-Gateway von A
- Annahme dieser Pakete durch die Firewall von A, da Auffassung als Antwort auf die durch A anfangs versendeten Pakete
- Von nun an: Paketannahme bei beiden Firewalls (!)
- Bereitstellung von IP mittels PPP-über-unseren-UDP-Tunnel

Lösung

- Versendung von UDP-Paketen von A an den NAT-Gateway von B
- Blocken dieser Pakete durch die Firewall von B (klar)
- Versendung von UDP-Paketen von B an den NAT-Gateway von A
- Annahme dieser Pakete durch die Firewall von A, da Auffassung als Antwort auf die durch A anfangs versendeten Pakete
- Von nun an: Paketannahme bei beiden Firewalls (!)
- Bereitstellung von IP mittels PPP-über-unseren-UDP-Tunnel

Lösung

- Versendung von UDP-Paketen von A an den NAT-Gateway von B
- Blocken dieser Pakete durch die Firewall von B (klar)
- Versendung von UDP-Paketen von B an den NAT-Gateway von A
- Annahme dieser Pakete durch die Firewall von A, da Auffassung als Antwort auf die durch A anfangs versendeten Pakete
- Von nun an: Paketannahme bei beiden Firewalls (!)
- Bereitstellung von IP mittels PPP-über-unseren-UDP-Tunnel

Aufbau der Proof-of-Concept-Implementierung

1. Gegenseitiges Senden von „Müll“-Paketen (zum „Austricksen“ der Firewalls)
2. Gegenseitiges Senden eines Acknowledgement-Pakets
3. Warten auf ACK-Paket
4. Entweder Binden von `STDIN` und `STDOUT` an den Socket und exec() eines Programms oder
   Relayen von Tastatureingaben zur Gegenseite und umgekehrt

Beispielanwendung

```
root@A # ./nat-udp.pl \
  --port=42000 \
  --peer=NAT-Gateway-von-B \
  --cmd="pppd updetach noauth passive notty \
        ipparam vpn 172.16.0.1:172.16.0.2" \
  --window=10

root@B # ./nat-udp.pl \
  --port=42000 \
  --peer=NAT-Gateway-von-A \
  --cmd="pppd nodetach notty noauth" \
  --window=10
```

Quellen

- `#parrot` auf `irc.perl.org` (Ursprüngliche Idee)
- `http://www.tldp.org/HOWTO/ppp-ssh/configclient.html#AEN305` (pppd-Parameter)
- `http://m19s28.vlinux.de/iblech/nat-udp.pl` (Implementierung)