Mit dem Linux-Router ins Internet

Michael Fuchs, Systemberater

Dieser Beitrag zeigt, wie man unter Berücksichtigung von Sicherheitsaspekten schnell einen direkten Zugriff von lokalen Rechnern aus auf das Internet ermöglicht. Dazu erfahren Sie zuerst etwas über die Grundlagen des Routing, Forwarding und Masquerading und dann über die Konfiguration eines internettauglichen Routers.

Router ermöglichen den Datenaustausch zwischen zwei Netzwerken (Subnetzen). Dabei dürfen die Subnetze eine unterschiedliche Hardwarebasis besitzen, wie das zum Beispiel bei Ethernet und Telefonleitung der Fall ist. Wichtig ist nur, daß beide Netze mit TCP/IP als Protokoll arbeiten. Als Grundsystem verwende ich Linux ab dem Kernel 2.2.x. Alle hier beschriebenen Konfigurationsschritte kann man unter SuSE-Linux bequem mit YaST einstellen. Auch wird vorausgesetzt, daß ein Internetanschluß über ein Modem oder mit ISDN vorhanden ist.

Um den Anschluß des gesamten Netzes ans Internet zu ermöglichen, müssen bei SuSE-Linux zuerst mit YaST zwei Einstellungen vorgenommen oder überprüft werden. Im Administrationsmenü muß die Konfigurationsdatei verändert werden. Stellen Sie sicher, daß die beiden Einträge *IP_DYNIP* und *IP_FORWARD* auf *yes* gesetzt sind. Der erste Parameter stellt sicher, daß der Router mit dynamischen IP-Adressen besser zurechtkommt. Der zweite legt fest, daß der Router Datenpakete aus dem lokalen Netz ins Internet weiterleitet.

Besitzen die Rechner im lokalen Netz private Adressen, hilft IP-Forwarding allein nichts, weil der erste Router im Internet die Anfragen der lokalen Rechner sofort verwerfen würde. Router im Internet sind so konfiguriert, daß sie Anfragen von oder an private Netz-Adressen nicht weiterleiten. In diesem Fall müßte der Server in der Anfrage die lokale IP-Adresse des Clients durch seine legale bei der Anwahl übermittelte IP-Adresse ersetzen, damit er die Daten lokal zustellen kann. Diese Aktion bezeichnet man als »Masquerading«.

Damit der Router alle Schalter auswerten kann, sollte man den Linux-Server nach der Änderung der Einstellungen rebooten, um die Einstellungen zu aktivieren.

Wenn die Routen richtig gesetzt sind, besteht jetzt eine direkte Verbindung zwischen allen Rechnern im lokalen Netz und dem Internet.

Auf alle Fälle sollte dann in der Datei »/etc/hosts« die IP-Nummer und der Name der im Netz vorhandenen Rechner stehen. Diese Datei ist mit einem Texteditor zu öffnen und zu editieren. Zum Beispiel sieht das dann so aus (bei einem Router und einem Client):

```
#etc/host
127.0.0.1           localhost
192.168.0.2         Router.Mydomain
192.168.0.3         Client.Mydomain
```

Hierbei handelt es sich somit um zwei Rechner, die sich im Netz mit der Netz-IP 192.168.0.0 befinden. Der Router heißt somit »Router«, ist Mitglied der Domain »Mydomain« und besitzt im Netz die IP-Nummer 192.168.0.2. Analog dazu besitzt der Client den Namen »Client«, befindet sich ebenfalls in der Domain »Mydomain« und wird über die IP-Adresse 192.168.0.3 angesprochen.

Wird nun an der Konsole des Rechners »Router« der Befehl

```
ping Client
```

eingegeben, müßte eine Rückmeldung der Pings erscheinen. Auf beiden Linux-Rechnern muß sich somit die gleiche Datei »etc/hosts« befinden. Sollte der Ping nicht durchkommen, muß die Netzwerkkonfiguration nochmals überprüft werden.

Router

Hier noch einmal als kurze Zusammenfassung: Ein internettauglicher Router muß also auf alle Fälle

- eine Routing-Information für das lokale Netz (meist »eth0«) besitzen,
- den Zugriff auf das Internet (»ppp0« oder »ippp0«) eingetragen haben und
- eine Default-Route auf das Internet-Device kennen.

Da die Dämonen beziehungsweise die Start-Skripten die Routen für »ppp0« beziehungsweise »ippp0« setzen, muß man nur darauf achten, daß diese eine

Default-Route setzen, damit man die Verbindung auch vernünftig nutzen kann.
Beim Masquerading versteckt sich ein ganzes lokales Netzwerk hinter einer einzigen IP-Adresse. Der Server fängt alle Datenpakete ab, die ins Internet weitergeleitet werden sollen, ersetzt die ungültige IP-Adresse des Absenders durch seine eigene gültige IP-Adresse und schickt das Paket weiter ins Internet. Der Client merkt von dieser doppelten Umsetzung nichts. Alle Internetdienste sind vom Client aus voll nutzbar.

Masquerading

Für die Umsetzung des Masquerading benötigen Sie eine Unterstützung im Kernel, Module für spezielle Funktionen und zum Steuern des Masqueradings das Programm »ipchains«. Der Standardkernel von SuSE-Linux enthält diese Unterstützung bereits.
»ipchains« steuert beziehungsweise kontrolliert die Paketfilterung im Kernel. Wobei es drei Arten von Firewall-Regeln (Chains) gibt:

- »Input«, wenn ein Paket an einem Interface ankommt.
- »Output«, bevor ein Datenpaket ein Interface verläßt.
- »Forward«, wenn ein Datenpaket von einem Interface zu einem anderen weiterleitet.

Jede Chain besteht aus einer Liste von Regeln. Die Regeln geben jeweils an, was zu tun ist, wenn der Header des Pakets einen bestimmten Aufbau besitzt. Als Ergebnis dieser Überprüfung ergibt sich für das Datenpaket eine der folgenden drei Möglichkeiten:

- »Accept«: der Kernel transportiert das Paket weiter.
- »Deny«: der Kernel verwirft das Paket.
- »Reject«: der Kernel verwirft das Paket mit einer Rückmeldung an den Absender.

In einer Forward-Chain ist zusätzlich auch »MASQ« erlaubt, womit man das Maskieren veranlaßt.
Fragt man die eingestellten Regeln mit *ipchains -L* ab, erhält man folgende Ausgabe:

```
Chain input  ( policy ACCEPT ) :
Chain forward  ( policy ACCEPT ) :
Chain output  ( policy ACCEPT ) :
```

Für alle drei Chains liegt die Default-Policy auf *ACCEPT*. Mit folgendem Befehl stellen Sie auf Masquerading um:

```
ipchains -P forward MASQ
```

Danach haben alle Rechner im lokalen Netz vollen Internet-Zugriff.
Bisher haben wir Masquerading nur aktiviert. Will man eine genauere Kontrolle über die Pakete haben, muß man etwas tiefer in den Umgang mit »ipchains« einsteigen. Hier einige Beispiele, wie man mit »ipchains« eine recht gute Firewall einrichten kann:

```
ipchains -P forward DENY
```

Setzt die Policy für die Forward-Chain auf *DENY*. Alle Pakete zwischen den Interfaces würde der Kernel also abweisen.

```
ipchain -A forward -s 192.168.0.0/24 -j MASQ
```

Hiermit fängt eine Regel an die Forward-Chains an. Der Kernel maskiert alle Pakete aus dem lokalen Netz mit der Adresse 192.168.0.x. Für diese Regel überprüft der Kernel den Absender (»-s«) und springt dann zu *MASQ* (»-j«). Somit wird das Paket maskiert.

```
ipchains -A input -s 127.0.0.1 -p icmp -j DENY
```

Damit kann man keinen Ping mehr von dieser Adresse ausführen, da das Antwortpaket nicht mehr durch die Firewall kommt. Wundern Sie sich nicht, wenn es lange dauert, bevor eine Fehlermeldung kommt, Sie können den Wartezustand aber mit [Ctrl]+[C] beenden. Mit *ipchains -D input 1* hebt man diese Regel wieder auf.

IP-Masquerading testen

Wenn nicht bereits geschehen, starten sie jetzt ihren Linux-Rechner wieder, um sicherzustellen, daß der Rechner normal in Betrieb ist und alle Masquerading-Regeln gestartet werden. Als nächstes überprüfen Sie noch einmal alle Verbindungen im internen LAN und zum Internet. Führen Sie dann den folgenden Testlauf durch:

1. Auf einem internen maskierten Rechner senden Sie einen Ping an seine eigene Adresse. Wenn der Rechner die Adresse 192.168.0.3 besitzt, rufen Sie *ping 192.168.0.3* auf. Damit läßt sich feststellen, ob TCP/IP auf dem Rechner korrekt läuft und die Netzwerkkarte richtig angesprochen wird.
2. Von einem maskierten Rechner testen Sie die interne Verbindung zur Ethernetkarte Ihres Linux-Masq-Servers. Im Beispiel wäre diese Prüfung mit *ping 192.168.0.2* durchzuführen. Dieser Test liefert – sofern er korrekt durchgeführt wird – den Nachweis, daß das Netzwerk und das Routing funktionsfähig sind.
3. Versuchen Sie nun von einem internen Rechner aus ein Ping an eine beliebige statische TCP/IP-Adresse im Internet zu senden. Eine gute Wahl ist der ftp-Server des Powerusers-BBS unter der statischen Adresse »24.2.168.186«. Kommt das Signal zurück, bedeutet das, daß Masquerading über das Internet funktioniert.
4. Als einen letzten Test sollten Sie von einem Ihrer maskierten Rechner einige WWW-Seiten aufrufen. Stellen Sie sicher, daß der Nameserver Ihres ISPs bei den Client-Rechnern eingetragen ist. Werden die Seiten aufgebaut, können Sie sicher sein, daß Masquerading ordentlich eingerichtet ist. ◆