Unsichtbarer Schutz mit Linux: Firewall auf Bridge-Ebene

Zugbrücke

Firewalls sind meist als Router implementiert, aber das muss nicht sein. Paketfilter im Bridge-Betrieb haben einige Vorteile: Sie lassen sich nachträglich in ein Netzwerk einfügen, ohne die Konfiguration der Netzkomponenten zu ändern. Unter Linux sorgen drei Befehle für flexibles Bridgewalling. Ralf Spenneberg

© Nick Lansley

Linux ist als stabile Firewall-Plattform fest etabliert. Mit Netfilter/IPtables [1] verfügt der Kernel über einen mächtigen Paketfilter. In der Regel kommt Netfilter auf einem Router zum Einsatz, es trennt in dieser klassischen Konfiguration zwei oder mehr Subnetze. Wer nachträglich in ein gewachsenes Netz eine Firewall einfügen will, muss daher dessen Infrastruktur entsprechend anpassen. Der Aufwand dafür kann enorm sein, da mit den geänderten IP-Adressen auch die Zugriffskontrolle von intern genutzten Diensten anzupassen ist.

Eine Bridge (besser bekannt unter dem Begriff Switch) lässt sich dagegen problemlos einfügen. Sie arbeitet auf OSI-Schicht 2 (Ethernet) und beachtet im Normalfall nur MAC-Adressen und nicht die IP-Nummern (siehe Kasten „Brückenbau“). Unter Linux lässt sich diese Eigenschaft trickreich nutzen, um die Firewall transparent in ein Netz einzufügen. Als Firewall wertet die Bridge dann sehr wohl auch höhere Protokollschichten aus (IP-Adressen, TCP-Ports). Davon bemerken die beteiligten Hosts jedoch nichts, wenn sie nur erlaubte Pakete versenden.

Kernelkonfiguration

Für den Linux-Kernel 2.4 haben Lennert Buytenhek und Bart de Schuymer ein Patch geschrieben, das die Firewall-Funktionalität im Bridge-Modus hinzufügt. Dieses Patch ist im Kernel 2.6 serienmäßig enthalten. Der Kernel muss lediglich richtig konfiguriert sein (siehe Abbildungen 1 und 2).

Relevant sind in der Netfilter-Gruppe alle Optionen, die im Zusammenhang mit der Bridge stehen, zum Beispiel die ARPtables-Unterstützung »IP_NF_ARPTABLES«, »IP_NF_ARPFILTER« und »IP_NF_ARP_MANGLE«. Diese Funktionen dürfen als Module oder als fester Kernel-Bestandteil übersetzt werden. Wichtig ist außerdem die Unterstützung des Physdev-Match »IP_NF_MATCH_PHYSDEV«. Diese Option ist ab dem Kernel 2.6 erforderlich, um beim Filtern der Pakete auf der Bridge das physikalische Interface zu prüfen.

Userspace-Werkzeuge

Ist der neue Kernel erfolgreich übersetzt und installiert, fehlen nur noch die Userspace-Werkzeuge. Während das »iptables«-Programm meist vorhanden ist, sind auf vielen Distributionen die Kommandos »arptables« und »ebtables« eigens nachzuinstallieren. Wer einen aktuellen 2.6er Kernel auf einer älteren Linux-Distribution betreibt, muss eventuell noch eine aktuellere Version des »iptables«-Befehls aufspielen.

Um die Bridge zu konfigurieren, ist das Bridge-Utils-Paket erforderlich [4]. Moderne Distributionen enthalten es bereits. Darin findet sich der Befehl »brctl«, den normalerweise nur Root einsetzen darf. Der Aufruf »brctl addbr br0« erzeugt die Bridge mit dem Namen »br0«. Der Befehl »ip link show br0« bestätigt, dass die Bridge existiert. Da sie einen Namen trägt, ist es sogar möglich, mehrere virtuelle Bridges in einem Linux-Rechner zu betreiben.

Die Bridge muss als Nächstes wissen, für welche Ethernet-Netzwerkkarten sie zuständig ist. Dazu sind per »brctl« die Interfaces zur Bridge hinzuzufügen:

```
brctl addif br0 eth0
brctl addif br0 eth1
```

Die Netzwerkkarten sollten zu diesem Zeitpunkt noch nicht konfiguriert sein, also weder den Zustand »UP« aufweisen noch über eine eigene IP-Adresse verfü-

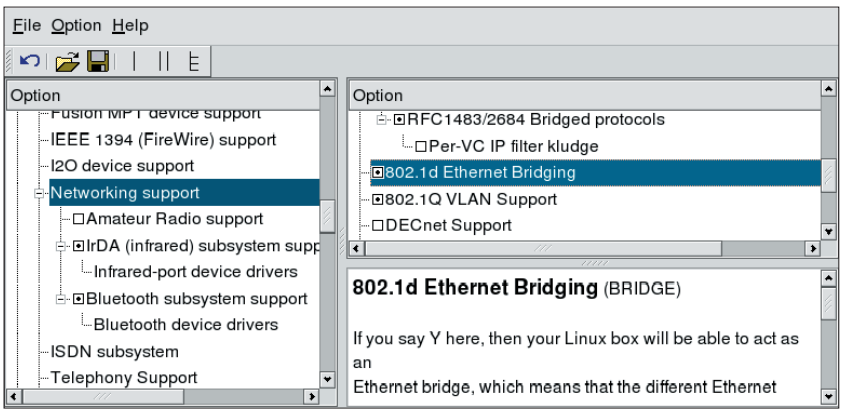

Abbildung 1: Um den Bridge-Modus im Kernel 2.6 zu aktivieren, muss unter »Networking Support« der Bereich »802.1d Ethernet Bridging« ausgewählt sein.

gen. Aktiviert werden sie erst, wenn sie zur Bridge gehören:

```
ip link set eth0 up
ip link set eth1 up
ip link set br0 up
```

Die Bridge ist nun einsatzbereit, wie »ip link show« zeigt (Abbildung 3). Sie leitet Pakete weiter und pflegt ihren ARP-Cache. Der verzeichnet, welche MAC-Adressen sie über welches Interface erreicht (siehe Kasten „Brückenbau“).

Bridgewalling

Wie jede andere Firewall kann die Bridge einen Regelsatz erhalten, der beschreibt, welche Pakete sie akzeptieren und welche verwerfen soll. Um dieses Bridgewalling zu definieren, stehen drei Befehle zur Verfügung:

- »iptables«
- »ebtables«
- »arptables«

Alle von der Bridge weitergeleiteten Pakete durchlaufen die »FORWARD«-Kette von Netfilter. Beim Einsatz des gewohnten »iptables«-Kommandos auf einer Bridge sind lediglich einige Besonderheiten zu berücksichtigen. Wenn eine Regel Pakete nur in einer bestimmten Richtung durch die Bridge passieren lassen soll, ist es wichtig, das Match »-m physdev« zu verwenden (siehe Tabelle 1). Dann kann die Policy prüfen, über welchen Bridge-Port ein Paket die Bridge erreicht oder ob es überhaupt von der Bridge verarbeitet wurde.

Bridgewall filtert auch nach TCP-Portnummer

Das folgende Beispiel soll den SSH-Verbindungsaufbau zum TCP-Port 22 auf der IP-Adresse 192.168.0.16 lediglich in einer Richtung zulassen. Der SSH-Server ist an »eth1« angeschlossen. Die Verbindungen dürfen nur von Clients ausge-

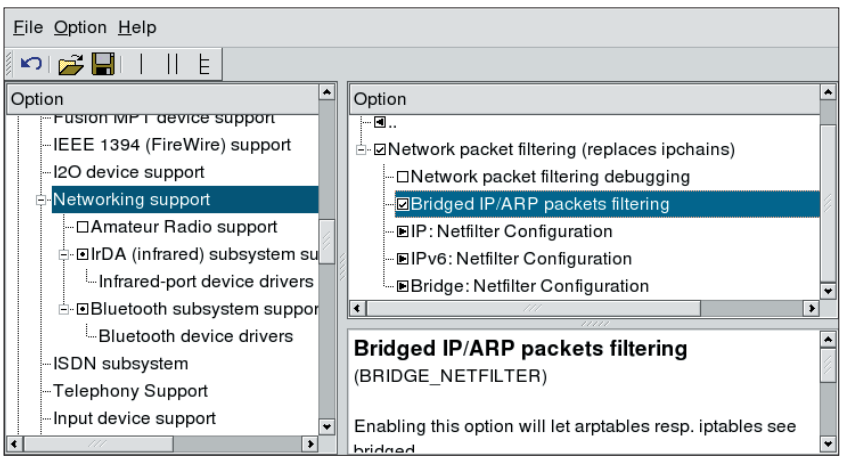

Abbildung 2: In der Netfilter-Kernelkonfiguration muss die Option »Bridged IP/ARP packets filtering« aktiviert sein, um Firewalling auf der Bridge zu erlauben.

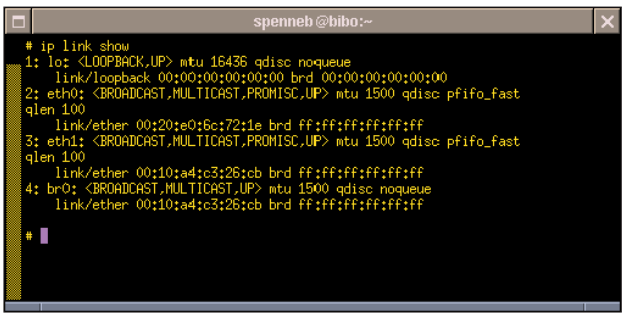

Abbildung 3: Die virtuelle Bridge ist in Betrieb. Die Ausgabe von »ip link show« zeigt nach »4: br0:« die Daten der Bridge.

hen, die an »eth0« angebunden sind. Zwei IPtables-Befehle setzen diese Policy um:

```
iptables -A FORWARD -m physdev ➥
  --physdev-in eth0 --physdev-out eth1 ➥
  --dport 22 -d 192.168.0.16 -m state ➥
  --state NEW -j ACCEPT
iptables -A FORWARD -m physdev ➥
  --physdev-is-bridged -m state ➥
  --state ESTABLISHED,RELATED -j ACCEPT
```

Das erste Kommando kümmert sich um den Verbindungsaufbau, den es nur in der gewünschten Richtung erlaubt. Dank des zweiten Befehls dürfen dann alle Pakete, die zu dieser Verbindung gehören, die Bridge passieren.

Adressensammler

Eine Bridge-Firewall wird häufig eingesetzt, wenn ein Administrator in einem gewachsenen Netzwerk zusätzliche Sicherheitsfunktionen benötigt. Er erspart sich damit die Änderung der Netzwerkinfrastruktur und der IP-Adressen. Einer der möglichen Einsatzorte liegt zwischen dem Internet-Zugangsrouter und dem internen Netz, wenn der Admin keinen Einfluss auf den Router hat oder wenn das Gerät über keine eigene Firewalling-Funktion verfügt. Ihre ganze Leistungsfähigkeit zeigen Bridgewalls aber erst, wenn sie bisher zusammengehörige Netzbereiche unterteilen.

Netz unterteilt

In diesem Fall befinden sich auf beiden Seiten der Bridge IP-Adressen, die sich nicht zu einem Bereich zusammenfassen lassen. Die Adressen sind zufällig verteilt. Hier hilft der »ipset«-Befehl den Überblick zu wahren: Er erzeugt einen Adressenpool, in dem der Admin beliebige IP-Adressen sammelt. Folgende Zeilen erzeugen den Pool namens »left« und fügen ihm drei IP-Adressen zu:

```
ipset -F; ipset -X; ipset -N left iphash
ipset -A left 192.168.0.5
ipset -A left 192.168.0.17
ipset -A left 192.168.0.18
```

Dieser neue Pool darf direkt in IPtables-Regeln stehen. Hierfür ist das Match »-m set« zuständig. Welcher Pool gemeint ist, steht in »--set *Name*«:

Tabelle 1: Physdev-Match

Option	Bedeutung
--physdev-in *Name*	Legt fest, über welchen Port der Bridge ein Paket gekommen sein muss, damit diese Regel zutrifft.
--physdev-out *Name*	Legt fest, über welchen Port ein Paket die Bridge verlassen muss, damit diese Regel zutrifft.
--physdev-is-in	Paket kam über ein Interface, das an einer Bridge angeschlossen ist.
--physdev-is-out	Das Paket wird den Rechner über ein Interface verlassen, das an einer Bridge angeschlossen ist.
--physdev-is-bridged	Das Paket durchläuft eine Bridge.

Listing 1: MAC-NAT

```
01 ebtables -t nat -A PREROUTING -p ARP --arp-ip-dst  -j arpreply --arpreply-mac 0:ff:90:2b:a6:16
02 ebtables -t nat -A PREROUTING -p IPv4 -d 0:ff:90:2b:a6:16 --ip-dst 192.168.0.16 -j dnat --to-dst
   fe:fd:0:0:0:1 --dnat-target ACCEPT
03 ebtables -t nat -A POSTROUTING -p IPv4 -s fe:fd:0:0:0:1 -j snat --to-src 0:ff:90:2b:a6:16
   --snat-target ACCEPT
```

```
iptables -A FORWARD -m physdev ➥
  --physdev-in eth0 --physdev-out eth1 ➥
  --dport 22 -m set --set left -m state ➥
  --state NEW -j ACCEPT
```

Neben den IP-Paketen sind vor allem ARP-Pakete ein lohnendes Ziel für Firewall-Regeln. Viele Angriffe innerhalb interner Netze bedienen sich gefälschter ARP-Anfragen und -Antworten [5].

ARPtables und EBtables

Der Befehl »arptables« ist für das Filtern von ARP-Paketen zuständig. Außerhalb des Bridge-Betriebs ist er lediglich in der »INPUT«- und »OUTPUT«-Kette sinnvoll, da ein Router keine ARP-Pakete weiterleitet. Auf einer Bridge kann ARPtables aber auch in der »FORWARD«-Kette arbeiten. Der Befehl ähnelt dem Kommando »iptables«. Er kennt ebenfalls die Targets »ACCEPT« und »DROP«, ein »REJECT« wäre dagegen sinnlos.

```
arptables -A FORWARD -s ! 192.168.0.15 ➥
  --destination-mac fe:fd:0:0:0:1 -j DROP
```

Dieser Aufruf verwirft alle ARP-Antwortpakete, die an den Rechner mit der MAC-Adresse »fe:fd:0:0:0:1« gerichtet sind, aber nicht vom Rechner mit der IP 192.168.0.15 stammen. ARP-Antworten teilen dem Anfrager mit, welche MAC-Adresse zu der angefragten IP-Adresse gehört. Damit erfährt »fe:fd:0:0:0:1« aus dem Netz auf der anderen Seite der Bridge lediglich die zu 192.168.0.15 gehörende MAC-Adresse.

Der Befehl »ebtables« ist deutlich mächtiger und erlaubt sogar ein NAT der MAC-Adressen auf der Bridge. So verhindert die Bridge, dass ein Angreifer die MAC-Adressen der Rechner an einem anderen Port erfährt. Die Bridge erwidert alle ARP-Anfragen mit ihrer eigenen

Der Autor

Ralf Spenneberg arbeitet als freier Unix/Linux-Trainer, Berater und Autor. Er veröffentlichte 2002 sein erstes Buch „Intrusion Detection für Linux-Server". Ende 2003 erschien sein zweites

Werk namens „VPN mit Linux". In wenigen Wochen wird sein drittes Buch „Intrusion Detection und Prevention mit Snort und Co." auf den Markt kommen.

MAC-Adresse und führt für alle IP-Pakete ein MAC-NAT durch. Mit dem ersten Kommando in Listing 1 antwortet die Bridge auf alle ARP-Anfragen, die zur IP-Adresse 192.168.0.16 die passende MAC erfahren wollen, mit ihrer eigenen MAC-Adresse (»0:ff:90:2b:a6:16«).

Nach »--arp-ip-dst« steht die IP-Adresse des zu schützenden Rechners hinter der Bridge. Die »--arpreply-mac« ist die MAC-Adresse der Bridge. Für das MAC-NAT der IP-Pakete sind zusätzlich die Zeilen 2 und 3 aus Listing 1 nötig. In diesem Beispiel ist 192.168.0.16 die zu schützende IP-Adresse hinter der Bridge. Dieser Rechner verfügt über die MAC-Adresse »fe:fd:0:0:0:1«.

Die weiteren Möglichkeiten des »ebtables«-Befehls sind in der sehr guten Dokumentation auf der EBtables-Homepage [2] erklärt.

In den Tiefen der Netze

Mit Bridgewalling erhält der Netzwerkadministrator eine neue Klasse von Paketfiltern, die seinen Einfluss auf die Schicht 2 ausdehnen. Dennoch dienen auch die höheren Protokollschichten als Entscheidungskriterium, welche Pakete die Firewall passieren dürfen. Besonders praktisch am Bridge-Betrieb ist, dass sich die Firewall transparent in vorhandene Netze einfügen lässt.

Bridgewalls ersetzen einen Hub, Switch oder ein Cross-over-Kabel. Wer einige Rechner innerhalb des internen Netzes hinter eine Firewall sperren muss, braucht dank Bridgewalling die Maschinen nicht umzukonfigurieren. *(fjl)* ■

Infos

[1] IPtables: [http://www.iptables.org]
[2] EBtables: [http://ebtables.sf.net]
[3] ARPtables: [http://ebtables.sf.net]
[4] Linux-Bridge: [http://bridge.sf.net]
[5] Achim Leitner und Thomas Demuth, „Angriffstechnik im lokalen Netz – ARP-Spoofing und -Poisoning“: Linux-Magazin 06/04, S. 34

Brückenbau

Bei einer Bridge (auch Switch genannt) handelt es sich um ein Netzwerkgerät, das gezieltes Forwarding von Netzwerkpaketen auf OSI-Layer 2 beherrscht. Hierzu lernt die Bridge sämtliche im lokalen Netz verwendeten MAC-Adressen und merkt sich, über welchen Anschluss (Interface, Port) sie den zugehörigen Rechner erreicht. Erhält die Bridge ein Paket, dessen Ziel-MAC-Adresse sie kennt, leitet sie das Paket nur an das passende Interface weiter und vermeidet damit überflüssige Übertragungen. Wenn die Bridge die Ziel-MAC-Adresse nicht kennt, sendet sie das Paket über jeden Anschluss.

MAC-Adressen lernen und vergessen

Alle von der Bridge gelernten MAC-Adressen zeigt der Befehl »brctl showmacs br0« an. Er listet die Einträge tabellarisch: Die erste Spalte enthält die Port-Nummer, über die ein Rechner angeschlossen ist, die zweite Spalte nennt dessen MAC-Adresse. Weitere Spalten enthalten zusätzliche Verwaltungsinformationen.

Um auf Änderungen zu reagieren, zum Beispiel wenn ein Rechner eine neue Netzwerkkarte erhält oder an anderer Stelle angeschlossen wird, verwirft die Bridge alte MAC-Adressen aus ihrer Forwarding-Datenbank. Wie lange eine MAC unbenutzt sein muss, bevor die Bridge sie vergisst, ist mit »brctl setageingtime br0 *Sekunden*« einstellbar.

Der interne Verwaltungsaufwand wäre unnötig hoch, wenn die Bridge jede veraltete MAC-Adresse sofort entfernen würde. Sie erklärt die Adresse daher zunächst für ungültig und entfernt in regelmäßigen Abständen alle ungültigen Einträge (Garbage Collector Interval). Dieser Abstand lässt sich mit dem Befehl »brctl setgcint br0 *Sekunden*« einstellen. Der Defaultwert ist 0 Sekunden.

Spanning Tree Protokoll

Moderne Switches erlauben mit dem Spanning Tree Protocol eine hochverfügbare Konfiguration. Wenn zwei oder mehr Switches zwei Teilnetze verbinden, ermitteln sie alle verfügbaren Wege von einem Netzwerk zu jedem anderen. Nach der Auswahl eines Root-Switch bestimmt dieser die aktiven und nicht aktiven Pfade im Netzwerk und übermittelt die Information an alle beteiligten Switches.

Die Switches blockieren alle nicht aktiven Pfade und Interfaces und verhindern so, dass ein Paket doppelt (auf zwei unterschiedlichen Wegen) in sein Zielnetzwerk gelangt (Abbildung 4). Fällt ein Switch aus, ermitteln die verbleibenden alle noch verfügbaren Pfade und umgehen das fehlerhafte Gerät.

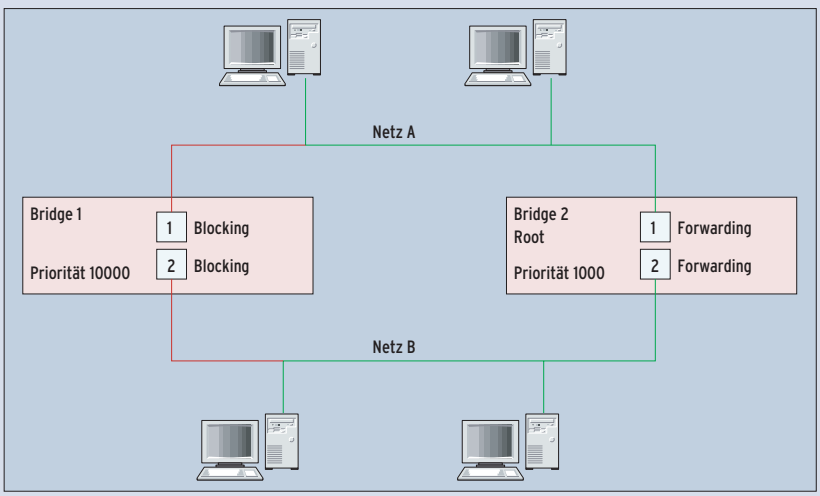

Abbildung 4: Die beiden Bridges 1 und 2 verbinden die Netze A und B. Per STP legt die Bridge mit der niedrigsten Priorität fest, auf welchem Weg die Pakete von A und B kommen dürfen.

Funktionstüchtig

Linux unterstützt das Spanning-Tree-Protokoll, allerdings muss es der Admin erst per »brctl stp br0 on« aktivieren. Die Priorität der Bridge lässt sich im Bereich von 0 bis 65535 frei definieren: »brctl setbridgeprio br0 *Priorität*«. Die Bridge mit der kleinsten Priorität übernimmt die Root-Funktion.

Bridges überwachen gegenseitig ihre Funktionstüchtigkeit, indem sie sich in regelmäßigen Abständen gegenseitig eine Hello-Nachricht zusenden. Der Abstand dieser Meldungen wird mit »brctl sethello br0 *Sekunden*« festgelegt. Der Befehl »brctl setmaxage br0 *Sekunden*« bestimmt, wie lange die anderen Bridges warten sollen, wenn die Hello-Meldungen ausbleiben. Nach der eingestellten Zeit geht das Bridge-Netzwerk davon aus, dass diese Bridge ausgefallen ist.

Neu angeschlossen darf eine Bridge erst nach einer Wartezeit damit beginnen, Pakete weiterzuleiten. In dieser Zeit muss sie prüfen, ob das STP-Protokoll im Netzwerk genutzt wird. Das Kommando »brctl setfd br0 *Sekunden*« ändert die Startverzögerung.

Auf einer filternden Bridge sollte das STP-Protokoll jedoch ganz deaktiviert sein: »brctl stp br0 off«. Die Firewall muss sich auf ihr Regelwerk verlassen und darf nicht durch gefälschte STP-Protokolle deaktivierbar sein.