Dokumentation

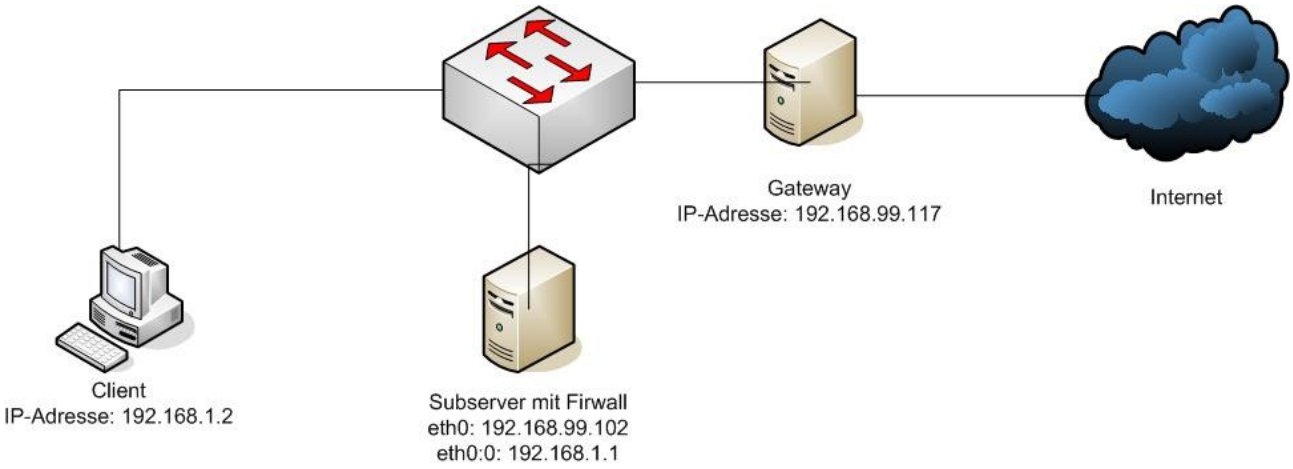
Konfiguration einer Firewall mit FireHOL

Inhalt:

1. Installation von FireHOL

```
apt-get install firehol
firehol-wizard > /etc/firehol/firehol.conf
```

2. Netzübersicht



3. Konfigurationsoptionen

Wichtigste Konfigurationsoptionen:

- interface, legt virtuelles Interface für FireHOL fest
  interface <real interface> <name> [optional rule parameters]
  Beispiel: interface eth0 intranet src 10.0.0.0/16

- router, gibt Quell- und Zielnetz an
  router <name> [optional rule parameters]
  Beispiel: router mylan inface ppp+ outface eth0

- policy, setzt die Standardpolicy für ein interface oder einen router
  policy <action>
  Beispiel: policy drop

- server, Dienst kann für ein interface oder einen router konfiguriert werden
  server <service> <action> [optional rule parameters]
  Beispiel: server smtp accept

- client, Konfiguriert zugriff auf einen Dienst
  client <service> <action> [optional rule parameters]
  Beispiel: client smtp accept

- route, Alias für server, kann jedoch nur für router benutzt werden
  route <service> <action> [optional rule parameters]
- masquerade, aktiviert NAT für ein Interface
  masquerade [reverse | interface] [optional rule parameters]
  Beispiel: masquerade
- **accept**, Akzeptiert Pakete
- **drop**, Verwirft Pakete ohne Rückmeldung

4. Anpassen der FireHOL Konfiguration

```
interface eth0 interface1 src "192.168.1.0/24" dst 192.168.1.1
# Konfiguriert das Interface eth0:0
      policy drop
      # Alle Pakete die nicht konfiguriert werden, werden verworfen
      masquerade # Aktiviert NAT für das 192.168.1.0 Netz
      # Jetzt werden die erlaubten Dienste konfiguriert:
      server cups accept # Drucker
      server dns accept
      server ftp accept
      server ICMP accept
      server icp accept # Squid
      server ident accept
      server nfs accept
      server squid accept
      server sunrpc accept
      server nis accept
      client all accept # Erlaubt alle Dienste für Subserver

interface eth0 interface2 src "192.168.99.0/24" dst 192.168.99.102
# Konfiguriert das Interface eth0 für das Netz 192.168.99.0
      policy drop
      # Alle Pakete die nicht konfiguriert werden, werden verworfen
      client all accept # Erlaubt alle Dienste für Subserver

interface eth0 interface3 src not "${UNROUTABLE_IPS} 192.168.99.0/24" dst
192.168.99.102
# Konfiguriert das Interface eth0 für Internet
      policy drop
      # Alle Pakete die nicht konfiguriert werden, werden verworfen
      client all accept # Erlaubt alle Dienste für Subserver

router router1 inface eth0 outface eth0 src "192.168.1.0/24" dst
"192.168.99.0/24"
# Routing zwischen 192.168.1.0 und 192.168.99.0
      route all drop # Pakete werden verworfen

router router2 inface eth0 outface eth0 src "192.168.1.0/24" dst not
"${UNROUTABLE_IPS} 192.168.99.0/24"
```

```
# Routing zwischen 192.168.1.0 und Internet
      route all accept # Pakete werden akzeptiert

router router3 inface eth0 outface eth0 src "192.168.99.0/24" dst
"192.168.1.0/24"
# Routing zwischen 192.168.99.0 und 192.168.1.0
      route all drop # Pakete werden verworfen
router router4 inface eth0 outface eth0 src "192.168.99.0/24" dst not
"${UNROUTABLE_IPS} 192.168.99.0/24"
# Routing zwischen 192.168.99.0 und Internet
      route all drop # Pakete werden verworfen
router router5 inface eth0 outface eth0 src not "${UNROUTABLE_IPS}
192.168.99.0/24" dst "192.168.1.0/24"
# Routing zwischen Internet und 192.168.1.0
      route all drop # Pakete werden verworfen
router router6 inface eth0 outface eth0 src not "${UNROUTABLE_IPS}
192.168.99.0/24" dst "192.168.99.0/24"
# Routing zwischen Internet und 192.168.99.0
      route all drop # Pakete werden verworfen
```

5. FireHOL-Optionen

start
: Firewall (iptables) wird konfiguriert

stop
: Firewall (iptables) wird beendet

try
: Firewall (iptables) wird gestartet und nach spätestens 30 Sekunden muss „commit“ eingegeben werden, ansonsten wird die alte Firewall wiederhergestellt. (Sehr nützlich bei Fernkonfiguration).

6. Überprüfen der Ports mittels nmap (Portscanner)

- von **Client 192.168.1.2**:

pc01:/nethome/pc01# nmap 192.168.1.1

Starting Nmap 4.11 (http://www.insecure.org/nmap/) at 2008-01-16 18:50 CET
Interesting ports on pc02.g1.loc (192.168.1.1):
Not shown: 1671 filtered ports
PORT STATE SERVICE
21/tcp open ftp
53/tcp open domain
111/tcp open rpcbind
113/tcp open auth
631/tcp closed ipp
707/tcp open unknown
836/tcp open unknown
2049/tcp open nfs
3128/tcp open squid-http
MAC Address: 00:0A:5E:4F:0E:27 (3COM)
Nmap finished: 1 IP address (1 host up) scanned in 19.219 seconds

- von **192.168.99.114**:
pc14:/home/pc14# nmap 192.168.99.102

Starting Nmap 4.11 (http://www.insecure.org/nmap/) at 2008-01-16 10:45 CET
All 1680 scanned ports on pc02.rdf.loc (192.168.99.102) are filtered
MAC Address: 00:0A:5E:4F:0E:27 (3COM)

Nmap finished: 1 IP address (1 host up) scanned in 36.041 seconds

7. Quellen
http://firehol.sourceforge.net/