

Analyse der Aufgabenstellungen

Die Firewall-Experimente sollen in einem virtuellen Netzwerk auf der Basis von uml (user mode linux) durchgeführt werden.

Ziele dieses Experimentes:

- Routingtabellen einstellen, damit die jeder Rechner mit jedem kommunizieren kann.
 1. Es soll vom internen Hosts an alle Rechner Ping möglich sein, allerdings von externen Hosts kein Ping möglich sein.
- SSH Verbindung auf den Server R3 zulassen
 1. Von den internen Hosts (R1, R7) soll ein ssh-Zugriff auf den Server R3 ermöglicht werden.
- Die Dienste http und FTP auf dem Server 43 für alle internen und externen Hosts freigegeben werden.
- Der Zugriff von R7 auf das Internet soll mit Hilfe von NAT realisiert werden

Routingtabellen

R1

Der Rechner 1 ist im „Network 1“ deswegen, es muss zu jeden anderen Networks außerhalb Network 6 eine Route eingefügt werden.

Route add -net „NW2 & NW3 & NW4 & NW5“/24 gw Rechner 2

R2

Der Rechner 2 funktioniert als Router zwischen Network 1, Network 2 und VPN (Network 5).

Route add -net NW4/24 gw Rechner 6

Route add -net NW3/24 gw Rechner 4

R3

Der Rechner 3 ist nur im „Network 2“ deswegen, es muss zu jeden anderen Networks außerhalb Network 6 eine Route eingefügt werden.

Route add -net NW1/24 gw Rechner 2

Route add -net NW3/24 gw Rechner 4

Route add -net NW5/24 gw Rechner 2

Route add -net NW4/24 gw Rechner2

R4

Der Rechner 4 funktioniert als Router zwischen Network 2, Network 3

```
Route add -net NW1/24 gw Rechner 2  
Route add -net NW5/24 gw Rechner 2  
Route add -net NW4/24 gw Rechner 2
```

R5

Der Rechner R5 stellt die Verbindung zum Internet her und der ist im Network 3 und 6.

```
Route add -net NW4/24 gw Rechner 6  
Route add -net NW2/24 gw Rechner 4  
Route add -net NW1/24 gw Rechner 4
```

R6

Der Rechner funktioniert als Router zwischen Network 4,5,6

```
Route add -net NW1/24 gw Rechner 2  
Route add -net NW2/24 gw Rechner 2
```

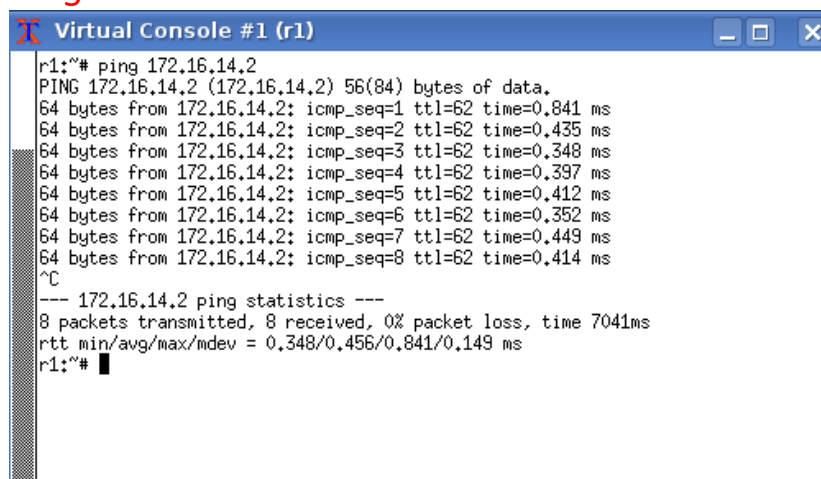
R7

Der Rechner ist im Network 4

```
Route add -net NW6/24 gw Rechner 6  
Route add -net NW5/24 gw Rechner 6  
Route add -net NW1/24 gw Rechner 6  
Route add -net NW2/24 gw Rechner 6
```

Die Überprüfung der Routingtabellen mit „ping“ und „traceroute“

Ping von R1 zu R7



```
Virtual Console #1 (r1)  
r1:~# ping 172.16.14.2  
PING 172.16.14.2 (172.16.14.2) 56(84) bytes of data.  
64 bytes from 172.16.14.2: icmp_seq=1 ttl=62 time=0.841 ms  
64 bytes from 172.16.14.2: icmp_seq=2 ttl=62 time=0.435 ms  
64 bytes from 172.16.14.2: icmp_seq=3 ttl=62 time=0.348 ms  
64 bytes from 172.16.14.2: icmp_seq=4 ttl=62 time=0.397 ms  
64 bytes from 172.16.14.2: icmp_seq=5 ttl=62 time=0.412 ms  
64 bytes from 172.16.14.2: icmp_seq=6 ttl=62 time=0.352 ms  
64 bytes from 172.16.14.2: icmp_seq=7 ttl=62 time=0.449 ms  
64 bytes from 172.16.14.2: icmp_seq=8 ttl=62 time=0.414 ms  
^C  
--- 172.16.14.2 ping statistics ---  
8 packets transmitted, 8 received, 0% packet loss, time 7041ms  
rtt min/avg/max/mdev = 0.348/0.456/0.841/0.149 ms  
r1:~#
```

Tcpdump von R1 zu R7

```
Virtual Console #1 (r1)
r1:~# ping 172.16.14.2
PING 172.16.14.2 (172.16.14.2) 56(84) bytes of data.
64 bytes from 172.16.14.2: icmp_seq=1 ttl=62 time=0.701 ms
64 bytes from 172.16.14.2: icmp_seq=2 ttl=62 time=0.552 ms
64 bytes from 172.16.14.2: icmp_seq=3 ttl=62 time=0.536 ms
64 bytes from 172.16.14.2: icmp_seq=4 ttl=62 time=0.689 ms
64 bytes from 172.16.14.2: icmp_seq=5 ttl=62 time=0.539 ms
64 bytes from 172.16.14.2: icmp_seq=6 ttl=62 time=0.398 ms
^C
--- 172.16.14.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5021ms
rtt min/avg/max/mdev = 0.398/0.569/0.701/0.103 ms
r1:~# █

Virtual Console #1 (r2)
r2:~# tcpdump -i eth2 -s 100
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth2, link-type EN10MB (Ethernet), capture size 100 bytes
08:22:33.843919 IP r1_0 > r7_0: ICMP echo request, id 14082, seq 1, length 64
08:22:33.844252 IP r7_0 > r1_0: ICMP echo reply, id 14082, seq 1, length 64
08:22:34.851703 IP r1_0 > r7_0: ICMP echo request, id 14082, seq 2, length 64
08:22:34.851986 IP r7_0 > r1_0: ICMP echo reply, id 14082, seq 2, length 64
08:22:35.855910 IP r1_0 > r7_0: ICMP echo request, id 14082, seq 3, length 64
08:22:35.856247 IP r7_0 > r1_0: ICMP echo reply, id 14082, seq 3, length 64
08:22:36.856684 IP r1_0 > r7_0: ICMP echo request, id 14082, seq 4, length 64
08:22:36.857151 IP r7_0 > r1_0: ICMP echo reply, id 14082, seq 4, length 64
08:22:37.863000 IP r1_0 > r7_0: ICMP echo request, id 14082, seq 5, length 64
08:22:37.863330 IP r7_0 > r1_0: ICMP echo reply, id 14082, seq 5, length 64
08:22:38.844367 arp who-has r6_1 tell r2_2
08:22:38.844694 arp who-has r2_2 tell r6_1
08:22:38.844699 arp reply r2_2 is-at 06:bd:43:c4:cc:37 (oui Unknown)
08:22:38.844720 arp reply r6_1 is-at f2:4e:de:3f:93:32 (oui Unknown)
08:22:38.864913 IP r1_0 > r7_0: ICMP echo request, id 14082, seq 6, length 64
08:22:38.865137 IP r7_0 > r1_0: ICMP echo reply, id 14082, seq 6, length 64
█

Virtual Console #1 (r6)
r6:~# tcpdump -i eth1 -s 100
tcpdump: verbose output suppressed, use -v or -vv for full protocol decode
listening on eth1, link-type EN10MB (Ethernet), capture size 100 bytes
08:22:33.788895 IP r1_0 > r7_0: ICMP echo request, id 14082, seq 1, length 64
08:22:33.789023 IP r7_0 > r1_0: ICMP echo reply, id 14082, seq 1, length 64
08:22:34.796603 IP r1_0 > r7_0: ICMP echo request, id 14082, seq 2, length 64
08:22:34.796761 IP r7_0 > r1_0: ICMP echo reply, id 14082, seq 2, length 64
08:22:35.800801 IP r1_0 > r7_0: ICMP echo request, id 14082, seq 3, length 64
08:22:35.801000 IP r7_0 > r1_0: ICMP echo reply, id 14082, seq 3, length 64
08:22:36.801577 IP r1_0 > r7_0: ICMP echo request, id 14082, seq 4, length 64
08:22:36.801850 IP r7_0 > r1_0: ICMP echo reply, id 14082, seq 4, length 64
08:22:37.807901 IP r1_0 > r7_0: ICMP echo request, id 14082, seq 5, length 64
08:22:37.808098 IP r7_0 > r1_0: ICMP echo reply, id 14082, seq 5, length 64
08:22:38.789296 arp who-has r2_2 tell r6_1
08:22:38.789284 arp who-has r6_1 tell r2_2
08:22:38.789522 arp reply r6_1 is-at f2:4e:de:3f:93:32 (oui Unknown)
08:22:38.789568 arp reply r2_2 is-at 06:bd:43:c4:cc:37 (oui Unknown)
08:22:38.809790 IP r1_0 > r7_0: ICMP echo request, id 14082, seq 6, length 64
08:22:38.809923 IP r7_0 > r1_0: ICMP echo reply, id 14082, seq 6, length 64
█
```

Traceroute von R1 zu R7

```
Virtual Console #1 (r1)
Last login: Mon May 17 07:12:11 UTC 2010 on tty1
Linux heitmann-virtual 2.6.34-rc7 #1 Sun May 16 18:21:32 CEST 2010 i686

The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
r1:~# traceroute 172.16.14.1
traceroute to 172.16.14.1 (172.16.14.1), 30 hops max, 40 byte packets
 1 * * *
 2 r6_2 (172.16.14.1) 29.131 ms 28.850 ms 28.738 ms
r1:~#
r1:~# traceroute 172.16.14.2
traceroute to 172.16.14.2 (172.16.14.2), 30 hops max, 40 byte packets
 1 r2_0 (172.16.11.2) 0.188 ms 0.082 ms 0.158 ms
 2 r6_1 (172.16.15.2) 0.156 ms 0.167 ms 0.122 ms
 3 r7_0 (172.16.14.2) 0.303 ms 0.184 ms 0.176 ms
r1:~#
```

Untersuchen der Ports mit einem Portscanner

Die Ports zwischen R1-R3, R5-R3, R7-R3 sind mittels „nmap“ gescannt.

```
Virtual Console #1 (r1)
64 bytes from 172.16.14.2: icmp_seq=5 ttl=62 time=0.539 ms
64 bytes from 172.16.14.2: icmp_seq=6 ttl=62 time=0.398 ms
^C
--- 172.16.14.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5021ms
rtt min/avg/max/mdev = 0.398/0.569/0.701/0.103 ms
r1:~# nmap -P0 -p1-99 172.16.12.2

Starting Nmap 4.62 ( http://nmap.org ) at 2014-12-15 08:23 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns_servers
Interesting ports on r3_0 (172.16.12.2):
Not shown: 96 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 1.935 seconds
r1:~#

Virtual Console #1 (r5)
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
r5:~# nmap -P0 -p1-99 172.16.12.2

Starting Nmap 4.62 ( http://nmap.org ) at 2014-12-15 08:23 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns_servers
Interesting ports on r3_0 (172.16.12.2):
Not shown: 97 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 11.483 seconds
r5:~#

Virtual Console #1 (r7)
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
r7:~# nmap -P0 -p1-99 172.16.12.2

Starting Nmap 4.62 ( http://nmap.org ) at 2014-12-15 08:23 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns_servers
Interesting ports on r3_0 (172.16.12.2):
Not shown: 96 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 1.929 seconds
r7:~#
```

Man kann sehen dass, FTP Port 21 und HTTP Port 80 erreichbar sind.

Einstellen der Policy

In den Firewalls R2, R4 und R6 die Policy der Ketten INPUT, OUTPUT und FORWARD auf DROP gestellt.

```
iptables -P FORWARD DROP
iptables -P INPUT DROP
iptables -P OUTPUT DROP
```

Auswirkungen:

Die Kommunikation über Router sind nicht mehr erfolgreich. Ping zwischen Rechnern über Router hat 100% Paketverlust. Mittels Traceroute bekommt man keine Informationen.

Ping erlauben

Um Ping zu erlauben an den Routern an den folgenden Ketten ein oder mehrere ACCEPTs hinzugefügt werden

- Von R5 soll kein Ping möglich sein
- Von den internen Netzen (also Host R1 und R7) Pings auf den Server (R3), allen Firewalls (R2, R4 und R6) und externen Hosts (R5) möglich sein sollen.

INPUT: Pakete für die internen Prozesse

FORWARD: Pakete, die von den internen Prozessen versandt werden

OUTPUT: Weiterzureichende Pakete

Zum Beispiel:

#Ping from Network 1 to Router 4

```
iptables -A INPUT -s 172.16.11.0/24 -p icmp --icmp-type ECHO-REQUEST -j ACCEPT
iptables -A OUTPUT -d 172.16.11.0/24 -p icmp --icmp-type ECHO-REPLY -j ACCEPT
```

#Ping from Network 2 to Network 3

```
iptables -A FORWARD -s 172.16.12.0/24 -d 172.16.103.0/24 -p icmp --icmp-type ECHO-REQUEST -j ACCEPT
iptables -A FORWARD -d 172.16.12.0/24 -s 172.16.103.0/24 -p icmp --icmp-type ECHO-REPLY -j ACCEPT
```

SSH auf den Server R3 in der DMZ zulassen

Von den internen Hosts (R1, R7) soll ein ssh-Zugriff auf den Server R3 ermöglicht werden, dazu muss der Port 22 freigegeben werden

Zum Beispiel:

#From Network 4 to Server (R3)

```
iptables -A FORWARD -p tcp --dport 22 -d 172.16.12.2 -j ACCEPT
```

```
iptables -A FORWARD -p tcp --sport 22 -s 172.16.12.2 -j ACCEPT
```

Mittels „nmap“ der ssh-Zugriff ist überprüft:

The image shows three terminal windows, each displaying the output of an nmap scan performed on the host 172.16.12.2. The windows are titled 'Virtual Console #1 (r1)', 'Virtual Console #1 (r5)', and 'Virtual Console #1 (r7)'. Each window shows the nmap command being executed, the scan progress, and the final results. The results indicate that the host is up and that ports 21/tcp (ftp), 22/tcp (ssh), and 80/tcp (http) are open. The scan was performed on 2014-12-15 at 08:23 UTC.

```
Virtual Console #1 (r1)
64 bytes from 172.16.14.2: icmp_seq=5 ttl=62 time=0.539 ms
64 bytes from 172.16.14.2: icmp_seq=6 ttl=62 time=0.398 ms
^C
--- 172.16.14.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5021ms
rtt min/avg/max/ndev = 0.398/0.569/0.701/0.103 ms
r1:~# nmap -P0 -p1-99 172.16.12.2

Starting Nmap 4.62 ( http://nmap.org ) at 2014-12-15 08:23 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns_servers
Interesting ports on r3_0 (172.16.12.2):
Not shown: 96 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 1.935 seconds
r1:~#
```

```
Virtual Console #1 (r5)
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
r5:~# nmap -P0 -p1-99 172.16.12.2

Starting Nmap 4.62 ( http://nmap.org ) at 2014-12-15 08:23 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns_servers
Interesting ports on r3_0 (172.16.12.2):
Not shown: 97 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ftp
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 11.483 seconds
r5:~#
```

```
Virtual Console #1 (r7)
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
r7:~# nmap -P0 -p1-99 172.16.12.2

Starting Nmap 4.62 ( http://nmap.org ) at 2014-12-15 08:23 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns_servers
Interesting ports on r3_0 (172.16.12.2):
Not shown: 96 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 1.929 seconds
r7:~#
```

Stateful Firewall

Die Dienste werden http und ftp auf dem Server R3 für alle internen und externen Hosts (R1, R7, und R5) freigegeben.

Http Port: 80

FTP Port: 21

Zum Beispiel:

#From Network 1 to Server (R3)

```
iptables -A FORWARD -m state --state ESTABLISHED,RELATED -j ACCEPT
```

```
iptables -A FORWARD -m state --state NEW -p tcp --syn --dport 80 -d 172.16.12.2 -j ACCEPT
```

```
iptables -A FORWARD -m state --state NEW -p tcp --syn --dport 21 -d 172.16.12.2 -j ACCEPT
```

Die Überprüfung der Ports mittels „nmap“

The image shows three screenshots of Nmap scan results in Virtual Console windows. The top-left window is titled 'Virtual Console #1 (r1)' and shows a successful scan of 172.16.12.2, identifying open ports 21/tcp (ftp), 22/tcp (ssh), and 80/tcp (http). The top-right window is titled 'Virtual Console #1 (r5)' and shows a similar scan of 172.16.12.2, also identifying open ports 21/tcp (ftp), 22/tcp (ssh), and 80/tcp (http). The bottom window is titled 'Virtual Console #1 (r7)' and shows a scan of 172.16.12.2, identifying open ports 21/tcp (ftp), 22/tcp (ssh), and 80/tcp (http). All three scans were performed on 2014-12-15 at 08:23 UTC and took approximately 1.9 seconds to complete.

```
Virtual Console #1 (r1)
64 bytes from 172.16.14.2: icmp_seq=5 ttl=62 time=0.539 ms
64 bytes from 172.16.14.2: icmp_seq=6 ttl=62 time=0.398 ms
^C
--- 172.16.14.2 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5021ms
rtt_min/avg/max/mdev = 0.398/0.569/0.701/0.103 ms
r1:~# nmap -P0 -p1-99 172.16.12.2

Starting Nmap 4.62 ( http://nmap.org ) at 2014-12-15 08:23 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns_servers
Interesting ports on r3_0 (172.16.12.2):
Not shown: 96 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 1.935 seconds
r1:~#
```

```
Virtual Console #1 (r5)
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
r5:~# nmap -P0 -p1-99 172.16.12.2

Starting Nmap 4.62 ( http://nmap.org ) at 2014-12-15 08:23 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns_servers
Interesting ports on r3_0 (172.16.12.2):
Not shown: 97 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 11.483 seconds
r5:~#
```

```
Virtual Console #1 (r7)
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

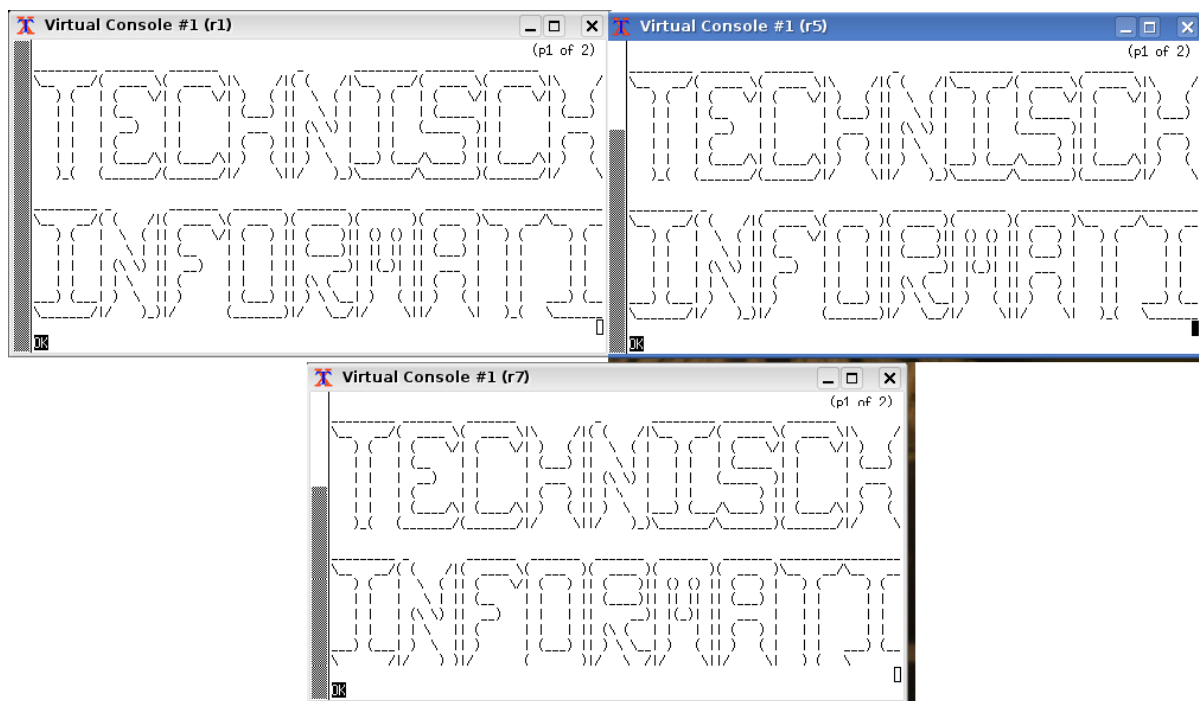
Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
r7:~# nmap -P0 -p1-99 172.16.12.2

Starting Nmap 4.62 ( http://nmap.org ) at 2014-12-15 08:23 UTC
mass_dns: warning: Unable to determine any DNS servers. Reverse DNS is disabled.
Try using --system-dns or specify valid servers with --dns_servers
Interesting ports on r3_0 (172.16.12.2):
Not shown: 96 filtered ports
PORT      STATE SERVICE
21/tcp    open  ftp
22/tcp    open  ssh
80/tcp    open  http

Nmap done: 1 IP address (1 host up) scanned in 1.929 seconds
r7:~#
```

Man kann sehen dass, FTP Port 21 und HTTP Port 80 erreichbar sind.

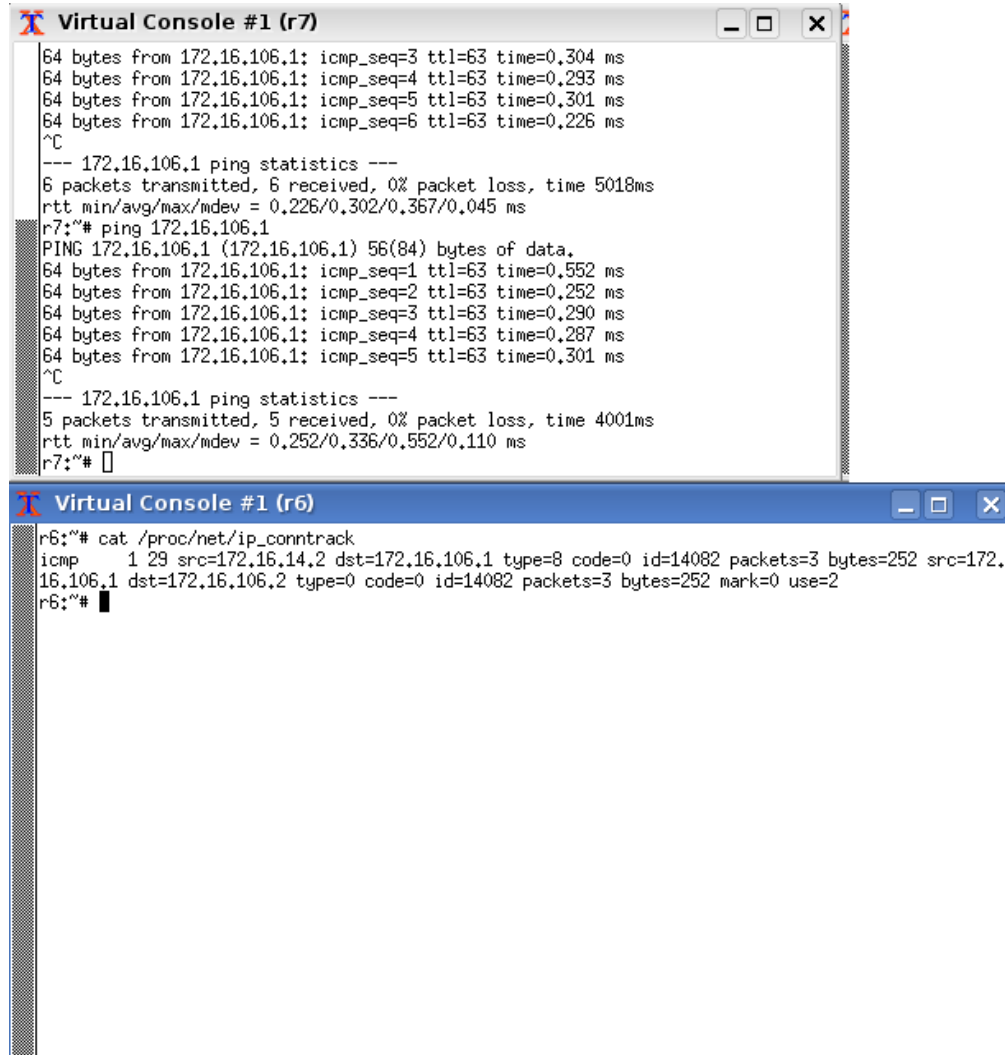
Testen die Funktionalität der Dienste http://r3_0 und ftp://r3_0/demo.txt



Network Address Translation (NAT)

Der Zugriff von R7 auf das Internet soll mit Hilfe von NAT realisiert werden.

`iptables -t nat -A POSTROUTING -o eth0 -j SNAT`



The image shows two screenshots of Virtual Console windows. The top window, titled 'Virtual Console #1 (r7)', displays the output of a ping command from router r7 to 172.16.106.1. It shows four successful ping attempts with varying times. Below this, it shows the ping statistics for 172.16.106.1, indicating 6 packets transmitted, 6 received, 0% packet loss, and a time of 5018ms. The bottom window, titled 'Virtual Console #1 (r6)', shows the output of the command 'cat /proc/net/ip_conntrack'. It displays a single entry for an ICMP packet from 172.16.14.2 to 172.16.106.1, with details such as type=8, code=0, id=14082, packets=3, bytes=252, src=172.16.106.1, dst=172.16.106.2, type=0, code=0, id=14082, packets=3, bytes=252, mark=0, and use=2.

```
Virtual Console #1 (r7)
64 bytes from 172.16.106.1: icmp_seq=3 ttl=63 time=0.304 ms
64 bytes from 172.16.106.1: icmp_seq=4 ttl=63 time=0.293 ms
64 bytes from 172.16.106.1: icmp_seq=5 ttl=63 time=0.301 ms
64 bytes from 172.16.106.1: icmp_seq=6 ttl=63 time=0.226 ms
^C
--- 172.16.106.1 ping statistics ---
6 packets transmitted, 6 received, 0% packet loss, time 5018ms
rtt min/avg/max/mdev = 0.226/0.302/0.367/0.045 ms
r7:~# ping 172.16.106.1
PING 172.16.106.1 (172.16.106.1) 56(84) bytes of data.
64 bytes from 172.16.106.1: icmp_seq=1 ttl=63 time=0.552 ms
64 bytes from 172.16.106.1: icmp_seq=2 ttl=63 time=0.252 ms
64 bytes from 172.16.106.1: icmp_seq=3 ttl=63 time=0.290 ms
64 bytes from 172.16.106.1: icmp_seq=4 ttl=63 time=0.287 ms
64 bytes from 172.16.106.1: icmp_seq=5 ttl=63 time=0.301 ms
^C
--- 172.16.106.1 ping statistics ---
5 packets transmitted, 5 received, 0% packet loss, time 4001ms
rtt min/avg/max/mdev = 0.252/0.336/0.552/0.110 ms
r7:~# 

Virtual Console #1 (r6)
r6:~# cat /proc/net/ip_conntrack
icmp      1 29 src=172.16.14.2 dst=172.16.106.1 type=8 code=0 id=14082 packets=3 bytes=252 src=172.
16.106.1 dst=172.16.106.2 type=0 code=0 id=14082 packets=3 bytes=252 mark=0 use=2
r6:~#
```

Nach dem Einstellen der NAT im Router kann man feststellen, dass der Rechner 5 die Pakete an Rechner 6 statt Rechner 7 schickt.