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

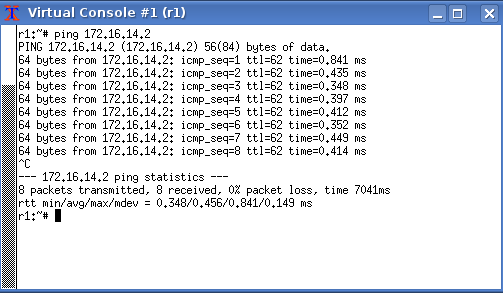
Route add –net NW5/24 gw Rechner 6

Route add –net NW1/24 gw Rechner 6

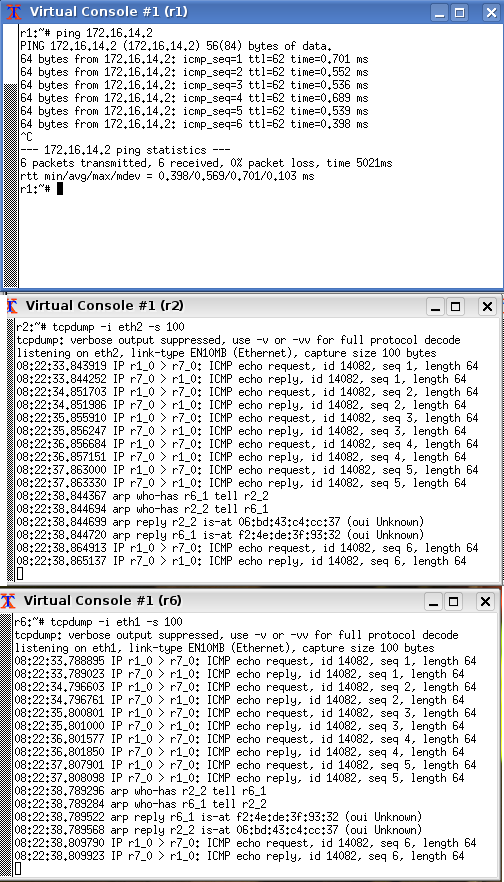
Route add –net NW2/24 gw Rechner 6

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

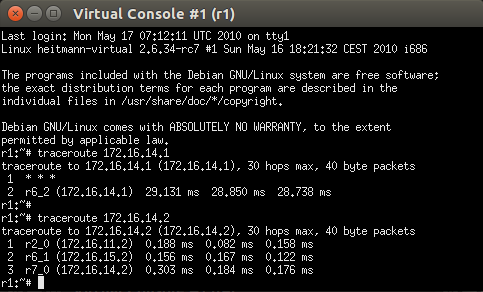
*Ping von R1 zu R7*



*Tcpdump von R1 zu R7*

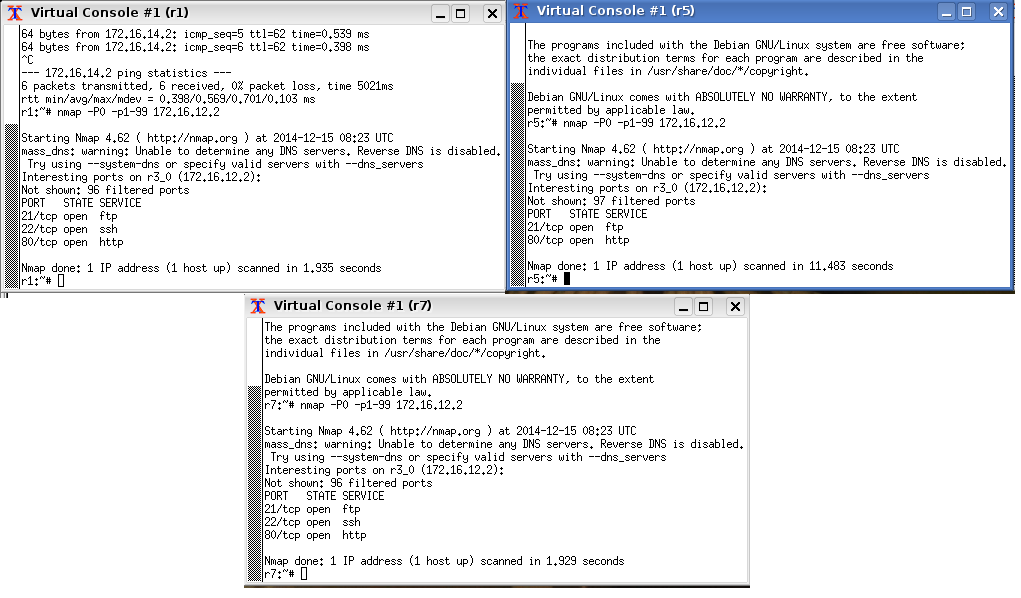


Traceroute von R1 zu R7



Untersuchen der Ports mit einem Portscanner

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



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 kommunikationen über Router sind nicht mehr erfolgreich. Ping zwischen Rechnern über Router hat 100% Paket verlust. 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 Beispeil:**

**#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

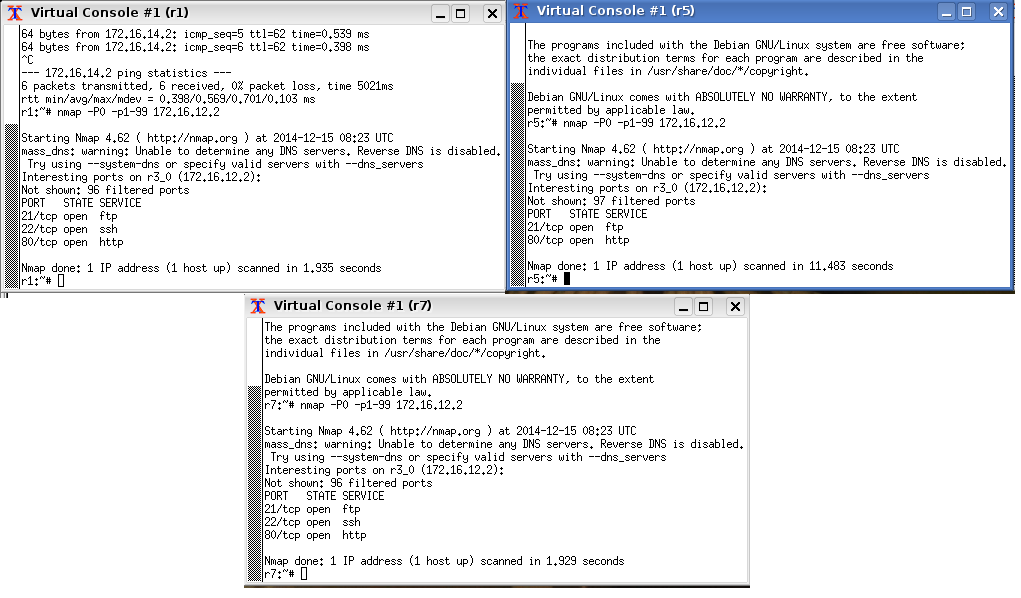
**Zum Beispiel:**

**#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:



### 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:**

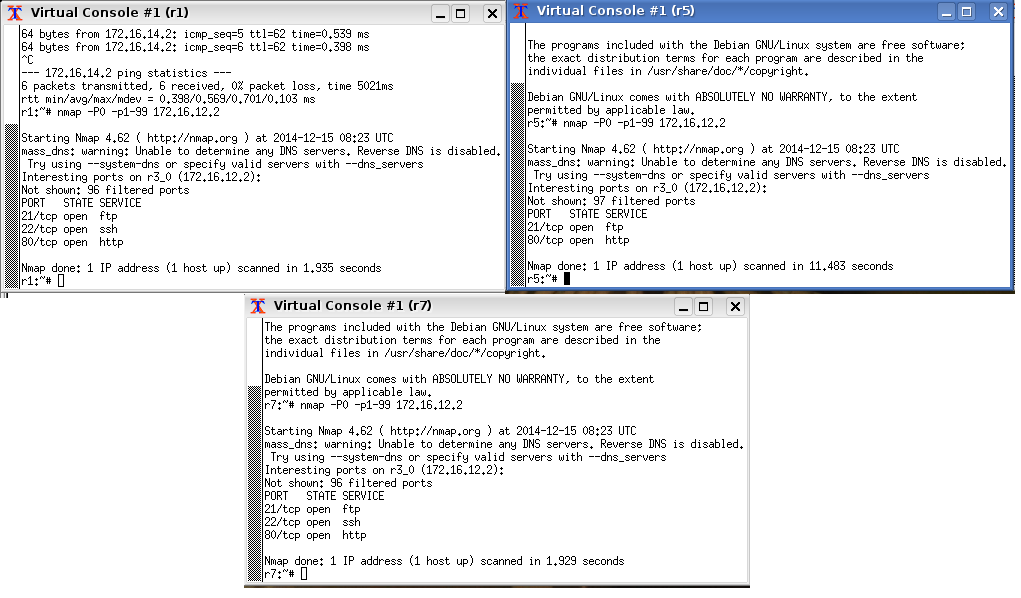
**#From Network 1 to Server (R3)**

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

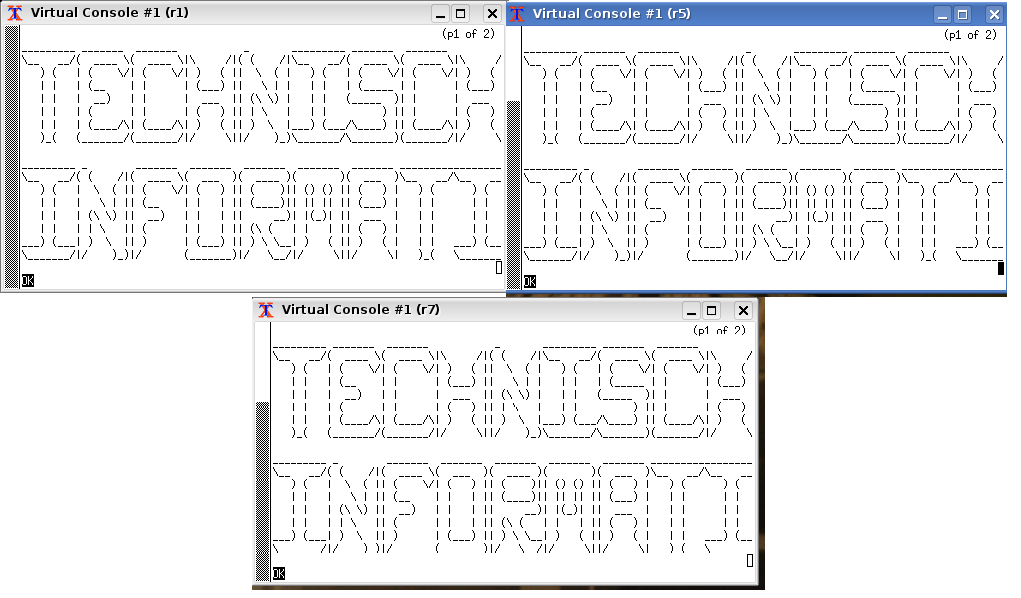
*Die Überprüfung der Ports mittels „nmap“*



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>

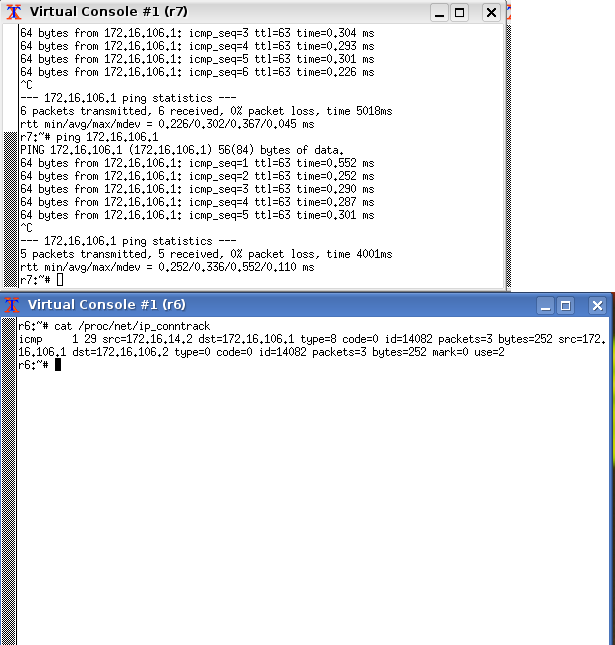




### Network Address Translation (NAT)

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

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



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