Installation einer Firewall
Gruppe 2

Server:	**eth0**	**192.168.99.117**	**rdf.loc**
SubServer:	**eth0**	**192.168.99.114**	**rdf.loc**
	eth0:0	**192.168.2.1**	**g2.loc**
Client:	**eth0**	**192.168.2.2**	**g2.loc**

Gruppe zwei wünscht ihnen viel Spaß beim Einrichten Ihrer Firewall

IAV3 - Jahrgang 06/08 der Rudolf-Diesel-Fachschule

1. Installation

→ apt-get install iptables ipmasq

2. Planung der FireWall

Philosophie: alle Zugänge/ Ports schließen DROP und Schritt für Schritt erlauben

SubServer soll nur mit Gateway kommunizieren können, der Rest soll verworfen werden.

Client soll nur mit Subserver kommunizieren können.

- → NFS in/out
- → DNS in/out
- → NIS in/out
- → http in/out
- → squid in/out

3. FwScript erstellen

Erstelle ein Script in **/etc/init.d/** mit dem Namen „fwscript".

→ **chmod 755 fwscript** um es ausführbar zu machen

Füge nun die geplanten Regeln in das Script ein und speichere es ab.

```
#Autoren: Andreas Beck, Maximilian Beck IAV0608
#Datum: 16.01.08
#####################################################################
# Definition der Variablen für iptables Konfiguration Subserver  #
#####################################################################
#Schnittstelle g2.loc 192.168.2.1
IFACE_INT=eth0

#Schnittstelle rdf.loc 192.168.99.114
IFACE_EXT=eth0

#Loopback device
IFACE_LO=lo

#Löschen vorhandener iptables
iptables -F

#Setzen der Default-Policies
iptables -P INPUT DROP
iptables -P FORWARD DROP
iptables -P OUTPUT DROP

#Datenverkehr auf Loopback ermöglichen (wird für XSERVER benötigt)
iptables -A INPUT -i $IFACE_LO -j ACCEPT
iptables -A OUTPUT -o $IFACE_LO -j ACCEPT

#####################################################################
#Subserver-Gateway Extern                                           #
#Problem dynamische Ports von NIS und NFS                           #
#Beim aktivieren der ersten zwei Regeln:                            #
# -> Dienste fkt. Nur Zugriff auf Internet fkt. Nicht               #
#Beim aktivieren der letzten drei Regeln:                           #
# -> Zugriff vom Clienten aufs Inet möglich, nicht über Squid       #
# -> Zugriff von anderen Rechnern möglich                           #
#####################################################################
#iptables -A INPUT -i $IFACE_EXT -s 192.168.99.117 -j ACCEPT
#iptables -A OUTPUT -o $IFACE_EXT -d 192.168.99.117 -j ACCEPT
#iptables -A INPUT -i $IFACE_EXT -j ACCEPT
#iptables -A OUTPUT -o $IFACE_EXT -j ACCEPT
#iptables -A FORWARD -o $IFACE_EXT -j ACCEPT
```

```
#####################################################################
#Subserver-Client Intern                                            #
#Problem dynamische Ports von NIS und NFS:                          #
#Keine Lösung gefunden, deshalb alles aus den Netzbereich g2.loc#
#erlaubt                                                            #
#####################################################################
#iptables -A INPUT -i $IFACE_INT -s 192.168.2.0/24 -j ACCEPT
#iptables -A OUTPUT -o $IFACE_INT -d 192.168.2.0/24 -j ACCEPT
#iptables -A FORWARD -o $IFACE_INT -j ACCEPT



#####################################################################
#Lösungsversuche / Test:                                            #
#####################################################################

#FTP-REGELN
#iptables -A OUTPUT -o $IFACE_INT -p TCP --dport 21 -j ACCEPT
#iptables -A INPUT -i $IFACE_INT -p TCP --sport 21 -j ACCEPT

#DNS-REGELN
#iptables -A OUTPUT -o $IFACE_INT -p UDP --dport 53 -j ACCEPT
#iptables -A INPUT -i $IFACE_INT -p UDP --sport 53 -j ACCEPT

#HTTP-REGELN
#iptables -A OUTPUT -o $IFACE_INT -p TCP --dport 80 -j ACCEPT
#iptables -A INPUT -i $IFACE_INT -p TCP --sport 80 -j ACCEPT

#RPCBIND-REGELN (Benötigt für NFS Portmap)
#iptables -A OUTPUT -o $IFACE_INT -p TCP --dport 111 -j ACCEPT
#iptables -A INPUT -i $IFACE_INT -p TCP --sport 111 -j ACCEPT

#AUTH-REGELN
#iptables -A OUTPUT -o $IFACE_INT -p TCP --dport 113 -j ACCEPT
#iptables -A INPUT -i $IFACE_INT -p TCP --sport 113 -j ACCEPT

#NFS-REGELN (Ermöglicht den Zugriff auf NFS-Dienst)
#iptables -A OUTPUT -o $IFACE_INT -p TCP --dport 2049 -j ACCEPT
#iptables -A INPUT -i $IFACE_INT -p TCP --dport 2049 -j ACCEPT
```

4. Symbolische Links für FwScript setzten

→ **update-rc.d fwscript defaults** erstellt symbolischen Link im RL

Jetzt den Rechner neu starten!

5. Probleme bei Debian Etch v3:

NFS(<=5) und NIS(<=v3.17) verwenden dynamisch Ports, dies führt zu Problemen.

→ Keine Bindung der dynamischen Ports möglich.

Subnetzstruktur äußerst ungeeignet, Firewall müsste auf dem Gateway liegen um Zugriff von außen zu sperren.