1 Vorbemerkungen

- Die beteiligten Rechner müssen mit der Linux-Partition *"BRV-Special"* gestartet werden, da zur Durchführung dieser Aufgabe z.T. administrative Rechte erforderlich sind. (Vgl. Hinweise im Anhang.)
- In Raum 765 gibt es neben dem Hochschulnetz (141.22.26.0/23) zwei laborinterne Netze: 192.168.17.0/24 bzw. 192.168.18.0/24 und 172.16.1.0/24, siehe Netzwerkplan.
- Sie brauchen grundsätzlich zwei Rechner. Dabei ist diese Rechnerzuordnung zu verwenden.
- Bei der Fehlersuche kann es nützlich sein, auf den beteiligten Rechnern den Netzwerkverkehr mit dem Sniffer (*wireshark*) aufzuzeichnen.
- Es wird erwartet, dass Sie sich vor dem Praktikum mit den hier verwendeten Befehlen vertraut gemacht haben. (Public-Bereich, Manual Pages, *iptables*-Tutorial.)
- Es ist ein Protokoll anzufertigen und zur Abnahme vorzulegen. Generell müssen alle Beobachtungen erläutert und alle Behauptungen begründet sein.

2 Paketfilterung (Firewalling)

Der Paketfilter wird mit dem Befehl *iptables* konfiguriert. Grundsätzlich kann eine Filterung zustandslos (stateless) oder zustandsorientiert (stateful) erfolgen.

Für die nachstehenden Szenarien ist jeweils ein Shellskript mit allen notwendigen Kommandos anzulegen, sodass die jeweilige Firewallkonfiguration jederzeit hergestellt werden kann. Achten Sie auf Vollständigkeit Ihrer Regeln, auch bezüglich der Policies!

→ *In nachfolgenden Fällen sollen alle nicht genannten Netze voll zugänglich bleiben!*
→ *Im 172er Netz gibt es keine Namensauflösung (DNS)!*

a) Auf einem Ihrer beiden Rechner soll der Zugang vom und zum Netzwerk 172.16.1.0/24 vollständig gesperrt werden.

b) Stellen Sie die Firewall des Rechners so ein, dass dort über das Netz 172.16.1.0/24 nur Ihr Chatserver genutzt werden kann. Alle anderen Verbindungen über dieses Netz sollen gesperrt sein.

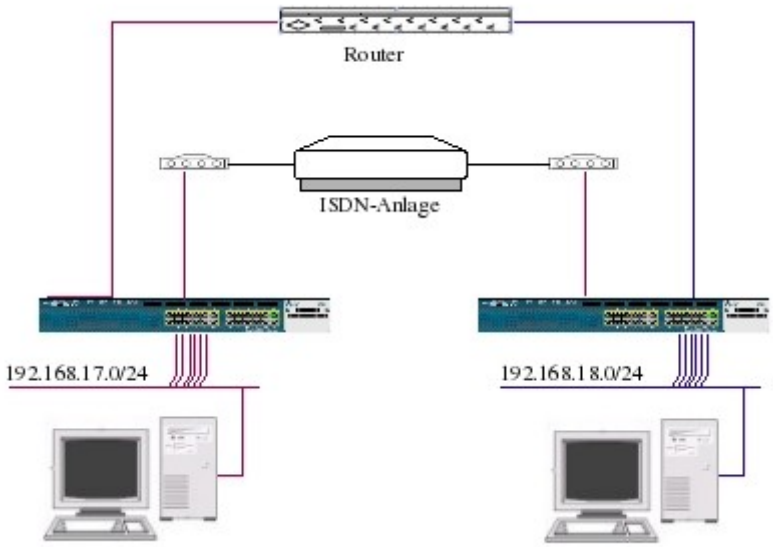
c) Konfigurieren Sie den Rechner so, dass er über das Netz 172.16.1.0/24 am Chat als Client teilnehmen, aber nicht als Server dienen kann. Andere Verbindungen über dieses Netz sollen ebenfalls gesperrt sein.

d) Stellen Sie die Firewall Ihres Rechners so ein, dass von dort ein *ping* auf andere Rechner/Geräte im Netz 172.16.1.0/24 möglich ist, nicht aber umgekehrt!

Wichtiger Hinweis: Nach kollektivem Löschen aller Regeln (Option *-F*), sind die Filesysteme hinter "*My Home*" und "*Public*" nicht mehr erreichbar. In diesem Fall müssen Sie – zusätzlich zu Ihren anderen Regeln – den Datenverkehr mit dem DNS-Server (141.22.192.100), dem Fileserver (*cifs.informatik.haw-hamburg.de*) und auch Ihrem lokalen Rechner (*localhost*) explizit freigeben! (U.a. wird *localhost* von der Fensteroberfläche benutzt!)

3 Routing

Das interne **192**er Netz besteht aus zwei Subnetzen. Ihre beiden Rechner befinden sich in unterschiedlichen Subnetzen. Die beiden Subnetze sind physikalisch über zwei Wege verbunden: Über einen Router und über eine ISDN-Anlage.



Konfigurieren Sie Ihre Rechner so, dass Sie den jeweils anderen Rechner im anderen Subnetz erreichen können. (Prüfung mit dem *ping*-Befehl). Dabei soll der gesamte Netzwerkverkehr entweder über den Router oder über die ISDN-Anlage laufen.
Was passiert, wenn Sie beim Weg über die ISDN-Anlage ein *ping* mit der Paketgrösse 1000 Byte durchführen? (Beobachtung im Sniffer und/oder Log von *ping*)

4 Sniffing

Stellen Sie zunächst die Firewalls der beteiligten Rechner so ein, dass Ihr Chatserver und -client über das Netz 172.16.1.0/24 wieder voll funktionieren.

a) Zeichnen Sie mit **wireshark** (Netzwerksniffer) den Netzwerkverkehr der TCP-Verbindung über das Netz **172.16.1.0/24** zwischen Ihrem Chatserver und einem Client auf einem anderen Rechner auf. Dokumentieren Sie Verbindungsaufbau und -abbau.

b) Setzen Sie dann auf Ihrem Chatserver-Rechner die Filterregeln für vollständige Abschottung (Teilaufgabe 2a) in Kraft. Zeichnen Sie erneut den Netzwerkverkehr auf. Wie reagiert der Chatclient?

c) Modifizieren Sie Ihre Filterregeln so, dass der Chatclient-Rechner ein Antwortpaket erhält, in dem das RESET-Flag gesetzt ist. Zeichnen Sie auch hierzu den Netzwerkverkehr auf. Wie reagiert der Chatclient?

Anhang

*Hinweise: Abgesehen von ping sind für nachfolgende Befehle in der Regel administrative Rechte notwendig. Dazu müssen diese mit dem **sudo**-Kommando gestartet werden!*

Beispiel : **sudo** `/usr/sbin/iptables -F`

Das sudo-Kommando ist nur für ausgewählte Programme zugelassen. Eigene Programme und Shellskripte können nicht mit sudo gestartet werden!

Detaillierte Informationen zu den Befehlen finden Sie in den Manual Pages.

route Aufruf (absoluter Pfad): `/sbin/route`

Lesen und Einstellen der Kernel-Routingtabelle.

Normalerweise wird eine Namensauflösung versucht. Ist dies nicht möglich, erfolgt nach Ablauf einer Wartezeit eine numerische Ausgabe. Mit der Option *-n* kann man die numerische Ausgabe direkt und ohne Wartezeit bekommen.
Anstelle der Netzmaske kann das Netz auch in Prefix-Schreibweise spezifiziert werden, also z.B. `172.16.0.0/16` statt `172.16.0.0 netmask 255.255.0.0`.

Hinweis: Lesender Zugriff ist auch ohne *sudo* möglich.

iptables Aufruf (absoluter Pfad): `/usr/sbin/iptables`

Lesen, Hinzufügen, Ändern und Löschen von Regeln für die Paketfilterung.

Hinweise: Normalerweise versucht *iptables* eine Namensauflösung. Ist diese nicht möglich, erfolgt nach einer Wartezeit eine numerische Ausgabe. Mit der Option *-n* kann man die numerische Ausgabe direkt und ohne Wartezeit bekommen.
Die Originaleinstellungen des Systems können auch mit dem Kommando

```
sudo /etc/init.d/SuSEfirewall2_setup restart
```

wiederhergestellt werden.

ping Aufruf: `ping` *<IP-Adresse oder Hostname>*

sendet eine ICMP-Echo-Anforderung an einen anderen Rechner und protokolliert die Echos.

wireshark Aufruf (absoluter Pfad): `/usr/bin/wireshark`

ist ein GUI-basiertes Tool zum Mithören ("Sniffen") des Netzwerkverkehrs, der über eine Netzwerkkarte abgewickelt wird. Es gibt viele Einstellmöglichkeiten, insbesondere zum Filtern der zu erfassenden sowie der im Fenster zu zeigenden Pakete.
(Weitere Informationen im Public-Bereich:
https://users.informatik.haw-hamburg.de/home/pub/staff/schulz/Rechnernetze/)