Aufgaben zum Thema UFW (Uncomplicated Firewall)	Name:	
	Klasse:	Datum:

Grundsätzliches

1. Beschreiben Sie ein Szenario, in welchem es wichtig ist, dass ein Webserver global verfügbar ist, andere Dienste nur innerhalb eines LAN erreichbar sind!
2. Warum müssen Sie `ufw` mit root-Rechten ausführen?
3. Interpretieren Sie die Statusanzeige (s. Box 4) ausführlich!

```
root@debian:~# ufw status verbose
Status: active
Logging: on (low)
Default: deny (incoming), allow (outgoing), disabled (routed)
New profiles: skip
```

Box 4: Ausführliche Anzeige des Status

Regeln erstellen

Schreiben Sie die jeweiligen `ufw`-Befehle mit korrekter Syntax auf!

4. Entfernen Sie alle http-bezogenen Regeln erlauben Sie den privaten Bereich der Netzwerkklasse C!
5. Sperren Sie anschließend den http-Zugriff für die Adresse 192.168.7.16!
6. Sperren Sie anschließend den http-Zugriff für den Bereich 192.168.9.0/24!
7. Überprüfen Sie, ob Sie folgende Statusanzeige (s. Box 4) erzielen!
8. Erläutern Sie die Regeln in Box 4!
9. Was ist zu tun, wenn Sie SSH ausschließlich aus privaten lokalen Netzen erlauben wollen? Erstellen Sie entsprechende Regeln! Die privaten Adressbereiche der Klassen A, B und C sind zu berücksichtigen.

```
root@debian:~# ufw status numbered
Status: active

     To                         Action      From
     --                         ------      ----
[ 1] 80/tcp                     DENY IN     192.168.7.16
[ 2] 80/tcp                     DENY IN     192.168.9.0/24
[ 3] 80/tcp                     ALLOW IN    192.168.0.0/16
[ 4] 22/tcp                     ALLOW IN    Anywhere
[ 5] 22/tcp (v6)                ALLOW IN    Anywhere (v6)
```

Box 4: Gewünschte Statusanzeige zu den Aufgaben 4 bis 8.

Netzwerkzugriffe sichten

10. Schreiben Sie die Syntax der Log-Datei heraus.
    Nähere Informationen finden Sie in der Ubuntu-Dokumentation zu UFW.
11. Entnehmen Sie dem Auszug der Logdatei (Box 3) folgende Informationen:
    Zeitstempel, Status, Bezeichnung der Netzwerkkarte, Quell- und Ziel-Ip-Adresse, Protokollvariante, Quell- und Ziel-Port!
12. Erlauben Sie Zugriffe auf den Webserver und verbieten Sie Zugriffe über SSH! Stellen Sie den Loglevel **medium** ein und testen Sie mit dem Webbrowser des Wirtsrechners und Putty Zugriffsversuche. Analysieren Sie anschließend die betreffenden Zeilen der Log-Datei!