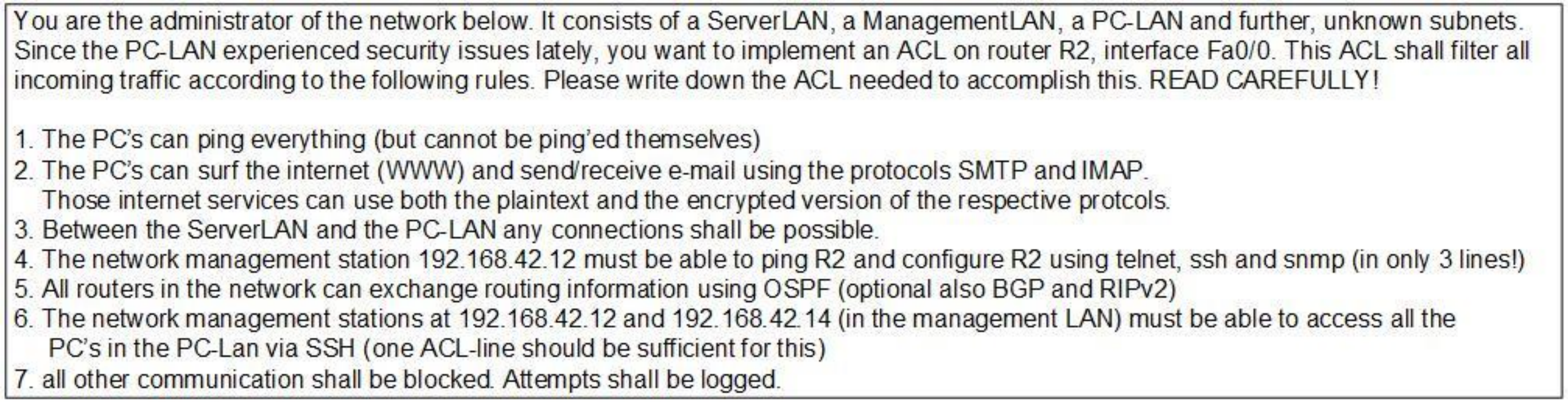
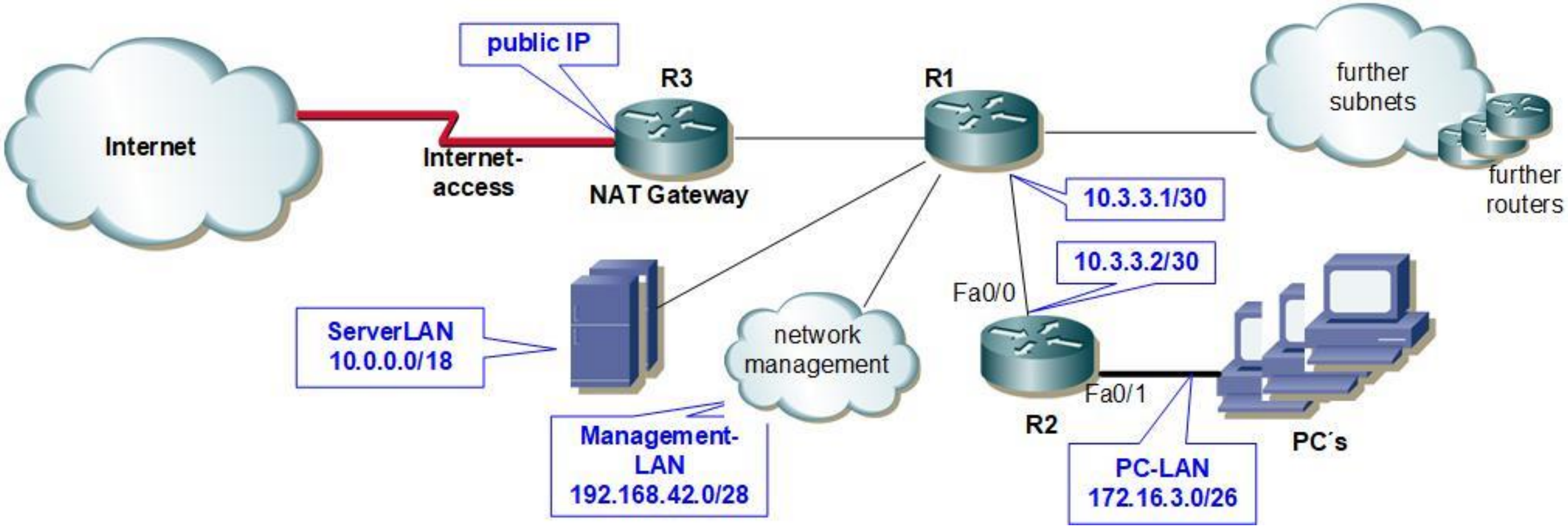
Übungen zu Kapitel 5: Netzsicherheit – ACL – NAT

Aufgabe: ACL Challenge



You are the administrator of the network below. It consists of a ServerLAN, a ManagementLAN, a PC-LAN and further, unknown subnets. Since the PC-LAN experienced security issues lately, you want to implement an ACL on router R2, interface Fa0/0. This ACL shall filter all incoming traffic according to the following rules. Please write down the ACL needed to accomplish this. READ CAREFULLY!

1. The PC's can ping everything (but cannot be ping'ed themselves)
2. The PC's can surf the internet (WWW) and send/receive e-mail using the protocols SMTP and IMAP.
   Those internet services can use both the plaintext and the encrypted version of the respective protcols.
3. Between the ServerLAN and the PC-LAN any connections shall be possible.
4. The network management station 192.168.42.12 must be able to ping R2 and configure R2 using telnet, ssh and snmp (in only 3 lines!)
5. All routers in the network can exchange routing information using OSPF (optional also BGP and RIPv2)
6. The network management stations at 192.168.42.12 and 192.168.42.14 (in the management LAN) must be able to access all the
   PC's in the PC-Lan via SSH (one ACL-line should be sufficient for this)
7. all other communication shall be blocked. Attempts shall be logged.



Name: _____**Rubaiya Kabir Pranti**_____ Matr.-Nr.: **11146364**

Bestimmen Sie die Konfiguration einer ACL für **Router R2**, **Interface Fa0/0** in **eingehender Richtung (in).**
(Betrachten Sie nur dieses Interface und diese Richtung auf Router R2. Alle übrigen notwendigen Paketfilterregeln werden hier nicht abgefragt.):

Example:
#PC-LAN network: 172.16.3.0
#Wildcard mask was calculated by subtracting inverse value of subnet mask from 255.255.255.255 which is achieved as 0.0.0.63

Configuration:

```
Router(config)# hostname R2
R2(config)# interface f0/0
```

#######Extended named ACL########

```
R2(config)# ip access-list extended in
```

2.1

```
R2(config-ext-nacl)# permit tcp any 172.16.3.0 0.0.0.63 eq 80 or eq www (PCs' can surf internet)
R2(config-ext-nacl)# permit tcp any 172.16.3.0 0.0.0.63 eq 443 (PCs' can surf internet with secure connection)
```

2.2

```
R2(config-ext-nacl)# permit tcp any 172.16.3.0 0.0.0.63 eq 587 (SMTP port with encryption from user to e-mail server)
R2(config-ext-nacl)# permit tcp any 172.16.3.0 0.0.0.63 eq 143 (IMAP port with insecurity from user to e-mail server)
R2(config-ext-nacl)#  permit tcp any 172.16.3.0 0.0.0.63 eq 993 (IMAP port with encryption/security from user to e-mail server)
```

3.

```
R2(config-ext-nacl)# permit ip 10.0.0.0 0.0.63.255 172.16.3.0 0.0.0.63 (From SERVER LAN to PC LAN where any connections are possible)
```

4.

```
R2(config-ext-nacl)#  permit icmp host 192.168.42.12 host 10.3.3.2 ( From network management station to R2 router)
R2(config-ext-nacl)# permit tcp host 192.168.42.12 host 10.3.3.2 eq 23 (Telnet port:23 is used from network management station to R2 router)
R2(config-ext-nacl)# permit tcp host 192.168.42.12 host 10.3.3.2 eq 22 (SSH port:22 is used from network management station to R2 router)
R2(config-ext-nacl)# permit udp host 192.168.42.12 host 10.3.3.2 eq 161 (SNMP port:161 is used from network management station to R2 router)
```

5.

```
R2(config-ext-nacl)# permit ip 10.3.3.0 0.0.0.3 10.3.3.0 0.0.0.3 eq 89 (All routers exchange info using 'ospf' where ospf:89)
R2(config-ext-nacl)# permit tcp 10.3.3.0 0.0.0.3 10.3.3.0 0.0.0.3 eq 179 (All routers exchange info using 'bgp' where bgp:179)
R2(config-ext-nacl)# permit udp 10.3.3.0 0.0.0.3 10.3.3.0 0.0.0.3 eq 520 (All routers exchange info using 'RIP' where RIP: 520)
```

6.

```
R2(config-ext-nacl)# permit tcp 192.168.42.0 0.0.0.15 172.16.3.0 0.0.0.63 eq 22 ( From network management station to PC-LAN using SSH:22)
R2(config-ext-nacl)# deny ip any any log (all other communications are being blocked by attempting log)
```