ANNEX A · PRACTICAL 3.8 · PORTS AND FIREWALLS

Name _____ **Group G =** _____ **Date** _____

Lines marked **[R]** go into your report.

TASK 1 · WHO IS LISTENING ON MY PC? (ALONE)

```
ss -tuln
python3 -m http.server 8080 &
ss -tlnp | grep 8080
nc -zv 127.0.0.1 8080
nc -zv 127.0.0.1 8081
grep -E "^(ssh|domain|https)\s" /etc/services
kill %1
```

Service	Port	TCP / UDP
SSH		
DNS		
HTTP		
HTTPS		

[R] Two listening sockets of your PC (address:port) — and who can reach each one? _____

[R] Message of `nc` for port 8080: _____ for port 8081: _____

PART A · A FIREWALL FOR YOUR GROUP'S ROUTER (WITH YOUR PARTNER GROUP H)

1 **Before.** From your PC, knock on your partners' router: `nc -zv -w 2 172.16.0.H 8291` (also `22` and `80`).

[R] Results: _____

2 In WinBox press **Safe Mode**. Interfaces → Interface List → Lists: create `WAN` and `LAN`. Members: `ether1` → `WAN`; `bridge-lan`, `vlan10`, `vlan20` → `LAN`.

3 IP → Firewall → Filter Rules, in this order (or type them in the Terminal):

```
/ip firewall filter
add chain=input action=accept connection-state=established,related,untracked
add chain=input action=drop connection-state=invalid
add chain=input action=accept protocol=icmp
add chain=input action=drop in-interface-list=!LAN
add chain=forward action=accept connection-state=established,related,untracked
add chain=forward action=drop connection-state=invalid
add chain=forward action=drop connection-state=new connection-nat-state=!dstnat \
in-interface-list=WAN
add chain=forward action=drop src-address=10.G.20.0/24 dst-address=10.G.10.0/24
```

4 **After.** Your partners knock again. **[R]** `nc` to 8291 now says: _____ `ping 172.16.0.G`: _____ `curl http://172.16.0.G:8080`: _____

5 Inside your group: the dev PC (`ether2`) pings the design PC (`ether3`): _____ and the other way: _____

[R] Which rule lets the answers through, and which one stops design? _____

DONE WHEN your partners cannot open WinBox on your router, they still see your page on 8080, and your PCs still have internet. Then leave Safe Mode.

PART B · RULE ORDER, STATE AND A HOST FIREWALL (ALONE, VIRTUAL LAB)

1 `G=3 containerlab deploy -t wan.clab.yml` · `ssh admin@clab-wan-r1`. Type yesterday's lines: the three addresses, the default route and the masquerade rule.

2 **Before.** From isp: `nc -zv -w 2 203.0.113.2 22` → _____ From pc2: `ping -c 2 10.G.10.11` → _____

3 Protect the router. **The first rule keeps your own `ssh` alive: do not skip it.**

```
/ip firewall filter
add chain=input action=accept in-interface=ether1 comment="lab management"
add chain=input action=accept connection-state=established,related,untracked
add chain=input action=accept protocol=icmp
add chain=input action=drop in-interface=ether2
```

[R] From isp, `nc` to port 22 now: _____ `ping 203.0.113.2`: _____

4 The order trap. Add:
`add chain=forward action=drop src-address=10.G.20.0/24 dst-address=10.G.10.0/24 comment="design-to-dev"`

pc2 pings pc1: _____ pc1 pings pc2 (`10.G.20.11`): _____ Now add
`add chain=forward action=accept connection-state=established,related,untracked`

pc1 pings pc2 again: _____ **[R]** Why does it still fail? _____

Fix it: `remove [find where comment="design-to-dev"]`, then add the drop rule again. **[R]** pc1 → pc2: _____

pc2 → pc1: _____

DONE WHEN dev can ping design, design cannot ping dev, and you can explain it with the word "established".

5 A host firewall, on isp. Start two servers (`cd /tmp; python3 -m http.server 80 &` and `python3 -m http.server 9090 &`), then:

```
ufw default deny incoming
ufw allow 80/tcp
ufw --force enable
```

[R] From pc1: `curl http://203.0.113.1` → _____ `nc -zv -w 2 203.0.113.1 9090` → _____

6 **[R]** `/ip firewall filter print` into the report, then `containerlab destroy -t wan.clab.yml --cleanup`.

Hand in `practical-3.8-surname.md` on Classroom before Monday 21/12 at 23:59: the **[R]** answers, the rule list, and in your own words: **"refused" or "timed out": what is the difference? And why does the order of rules matter?**

Marks (10): Task 1: 1 · Part A: 3 · Part B order trap and `ufw`: 3 · explanation: 2 · clear report: 1.

EXIT TICKET (ALONE, NO NOTES)

1. HTTPS normally uses: A · port 22, TCP B · port 53, UDP C · port 443, TCP D · port 8291, UDP
2. `ss -tln` shows `127.0.0.1:631`. That service can be reached:
   A · only from the same machine B · from the whole LAN C · from the internet D · by nobody
3. TCP, compared with UDP: A · is always faster B · sets up a connection and resends what is lost C · has no ports D · is only for video
4. A firewall starts with "accept established, related" so that:
   A · the router is faster B · pings are blocked C · new connections from the WAN enter D · answers to conversations started from inside can come back
5. `nc` says "timed out" instead of "refused". Most likely:
   A · a firewall dropped the packet without answering B · nobody listens on that port C · the port is UDP D · DNS failed