

ISA 656, Quiz (Extra Credit)

1) Assume you have the following firewall policy:

Action	prot	Source	Destination	Source port	Destination port
ACCEPT	UDP	129.174.113.0/25	129.174.17.0/25	*	53
REJECT	TCP	129.174.113.0/28	129.174.17.0/25	*	22
ACCEPT	TCP	129.174.113.0/25	129.174.17.0/25	*	22
ACCEPT	TCP	127.0.0.1	129.174.17.18	*	6000
REJECT	TCP	0.0.0.0/0	129.174.17.18	*	6000
ACCEPT	TCP	0.0.0.0/0	129.174.17.0/25	*	80
REJECT	TCP	0.0.0.0/0	129.174.17.0/25	*	80
ACCEPT	UDP	0.0.0.0/0	129.174.17.2	*	53
ACCEPT	TCP	0.0.0.0/0	129.174.17.3	*	22
ACCEPT	TCP	0.0.0.0/0	129.174.17.0/24	*	1024:65535
ACCEPT	TCP	129.174.17.0/25	0.0.0.0/0	*	*
ACCEPT	UDP	129.174.17.0/25	0.0.0.0/0	*	*
DENY	ALL	0.0.0.0/0	0.0.0.0/0	*	*

a) Identify any policy redundancies.

b) Assuming that the network we try to protect is 129.174.17.0/24, what are the services and corresponding hosts that are accessible from the outside?

c) Show what would happen to the following packets under the following tie-breaking strategies: first match (top-down) and last match (bottom up). For the bottom-up evaluation, ignore the last rule.

```
+-----+-----+-----+-----+
| UDP | s:128.174.113.129:22 | d:129.174.17.2:1024 | data...|
+-----+-----+-----+-----+
```

```
+-----+-----+-----+-----+
| UDP | s:129.174.17.3:53 | d:150.140.112:530 | data...|
+-----+-----+-----+-----+
```

```
+-----+-----+-----+-----+
| UDP | s:129.174.113.2:1122 | d:150.140.119.3:53 | data...|
+-----+-----+-----+-----+
```