

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.

Answer:

Typically, when evaluating redundancies or conflicts, and no approach is specified (top-down or bottom-up), a redundancy is any rule that is completely encompassed by another rule, i.e. if the redundant rule is removed, there is no difference in firewall behavior on a packet.

On the other hand, two rules conflict when they have different actions and there are packets can match both rules (i.e. they overlap fully or partly).

In this quiz, there are no redundant rules in this policy. There are rule overlaps. However, there are conflicts, for instance rules 6 and 7, but no redundant rules.

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?

Answer:

For the network 129.174.17.0, we protect hosts 129.74.17.1 to 129.174.17.255.

- DNS (UDP 53): Rule #1, #8
- SSH (TCP 22): Rule #3, #9
- Web/HTTP (TCP 80): Rule #7
- Ports 1024:65535 except 6000: Rule #10, minus #5

Rules 1 and 3 give access to a limited number of sources (129.174.113.0/25) outside of the protected network to a limited range of internal hosts. Rule 2 denies access to a limited sources outside (129.174.113.0/28) a limited range of hosts in the internal network. Rule 5 denies access from all sources to a single host’s XWindows service on the protected network.

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...|
+----+-----+-----+-----+-----+

```

Answer:

- | | Top-Down | Bottom-Up |
|------|-----------------------|-----------------------|
| i. | Deny by Rule 13 | Catch-all |
| ii. | Drop - Invalid packet | Drop - Invalid packet |
| iii. | Deny by Rule 13 | Catch-all |

When a packet doesn’t match, it is evaluated by the default firewall policy (that we do not know beforehand). This is the “Catch-all” policy and it is not the same for all firewalls but it is usually “Deny”.