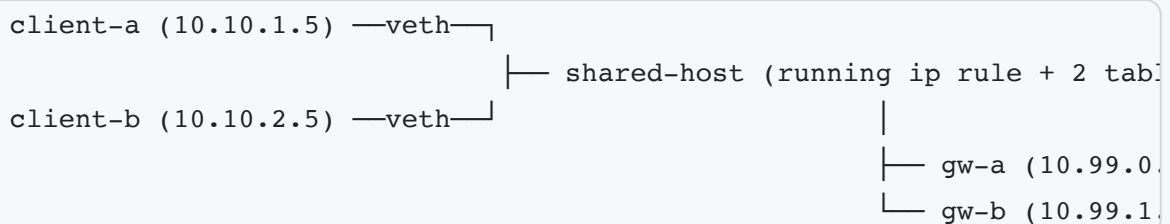


Homework — Lesson 03

~30 min · Three tasks · Uses ip netns + iptables mangle

Task 1 — Source-based routing across 3 namespaces

Build the following topology on a single host:



1. Create 5 namespaces: `client-a`, `client-b`, `shared-host`, `gw-a`, `gw-b`.
2. Connect them with veth pairs. Assign IPs as shown.
3. On `shared-host`, enable IPv4 forwarding.
4. Add `ip rule from 10.10.1.0/24 lookup 100` and `ip rule from 10.10.2.0/24 lookup 200`.
5. Populate table 100 with a default via `gw-a`; table 200 via `gw-b`.
6. Ping a "remote" IP from each client through the shared host.

Self-check:

- `ip route get 8.8.8.8 from 10.10.1.5` resolves via `gw-a`.
- `ip route get 8.8.8.8 from 10.10.2.5` resolves via `gw-b`.
- `tcpdump` on each gateway sees only its expected client.

Task 2 — fwmark-based routing

On a single namespace (or your host):

1. Add an iptables MANGLE rule in OUTPUT: mark all outbound SSH (tcp/22) traffic with `0x42`.
2. Add an `ip rule fwmark 0x42 lookup 300`.
3. Populate table 300 with a default via a different gateway than your normal one.
4. Verify with `ip route get 8.8.8.8 mark 0x42`.

Self-check:

- `iptables -t mangle -L OUTPUT -v -n` shows your MARK rule.
- `ip rule show` shows your fwmark rule.
- `ip route get 8.8.8.8 mark 0x42` resolves through table 300.

Task 3 — CONNMARK persistence verification

Building on Task 2's setup, add the three-rule CONNMARK chain:

1. Add `-j MARK --set-mark 0x42` on NEW packets (conntrack state NEW).
2. Add `-j CONNMARK --save-mark`.
3. Add `-j CONNMARK --restore-mark` BEFORE the MARK rule so subsequent packets get the mark before routing.
4. Open a long-lived TCP connection (e.g. `nc -lk 9999` on one namespace and `nc <ip> 9999` on another).
5. Run `conntrack -L | grep mark` while the connection is open.

Self-check:

- `conntrack -L` shows the connection entry with `mark=0x42`.

- After typing some data into `nc` on the client side, the response on the server side travels through the policy-routing table — verified by `tcpdump` on the alternate gateway namespace.
- Restarting `nc` creates a new conntrack entry which also gets the mark.

[View solutions →](#)