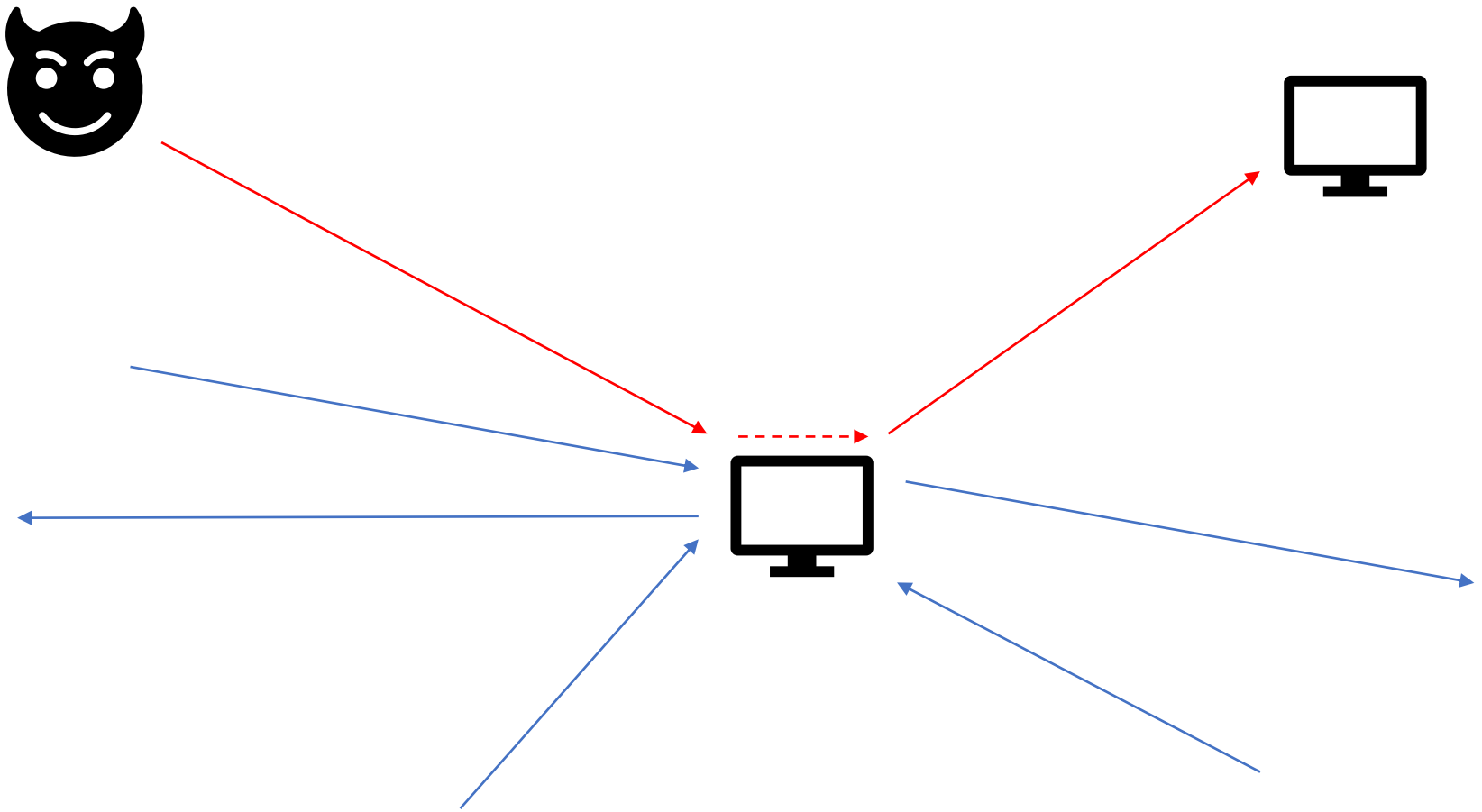
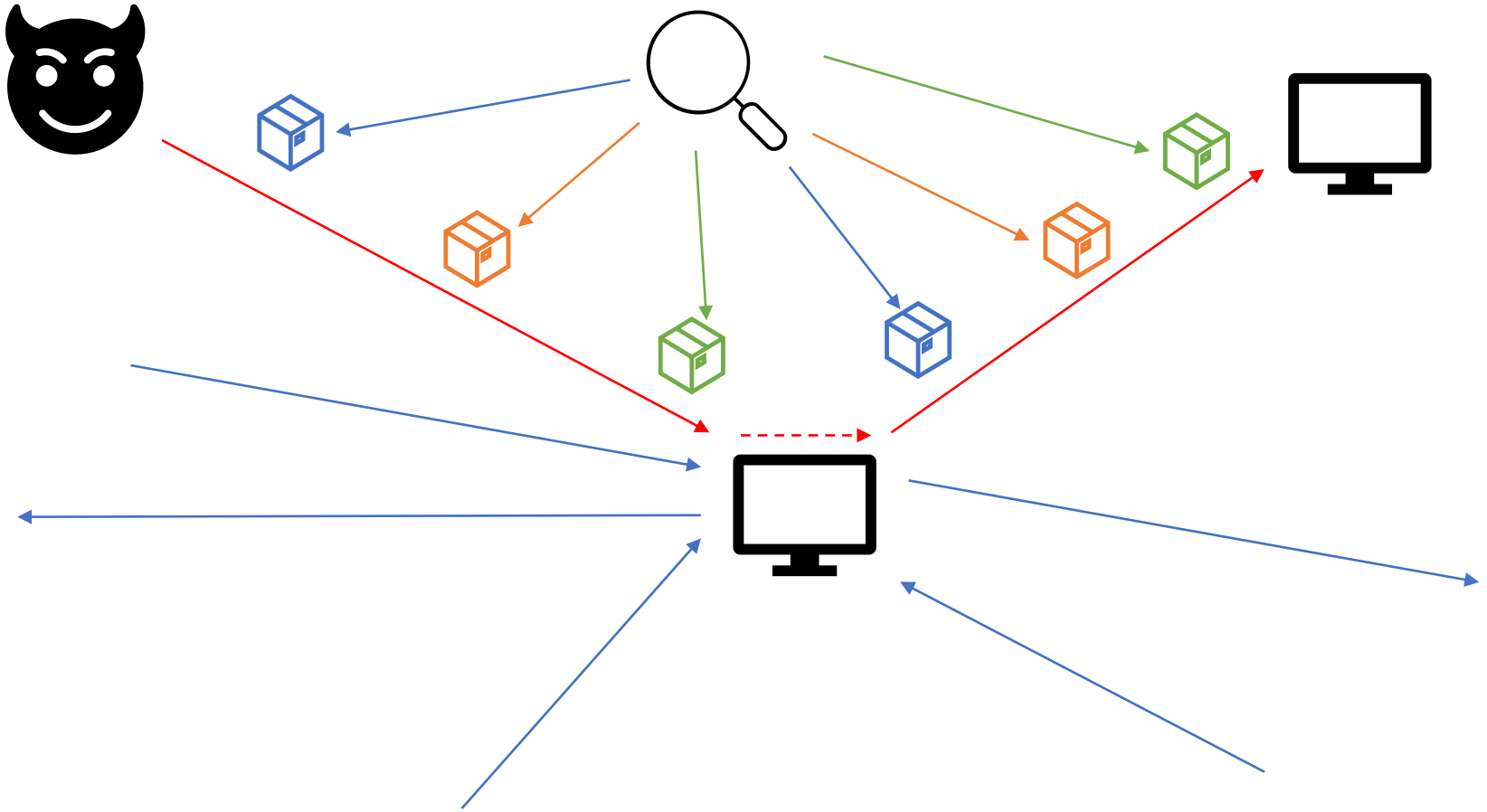
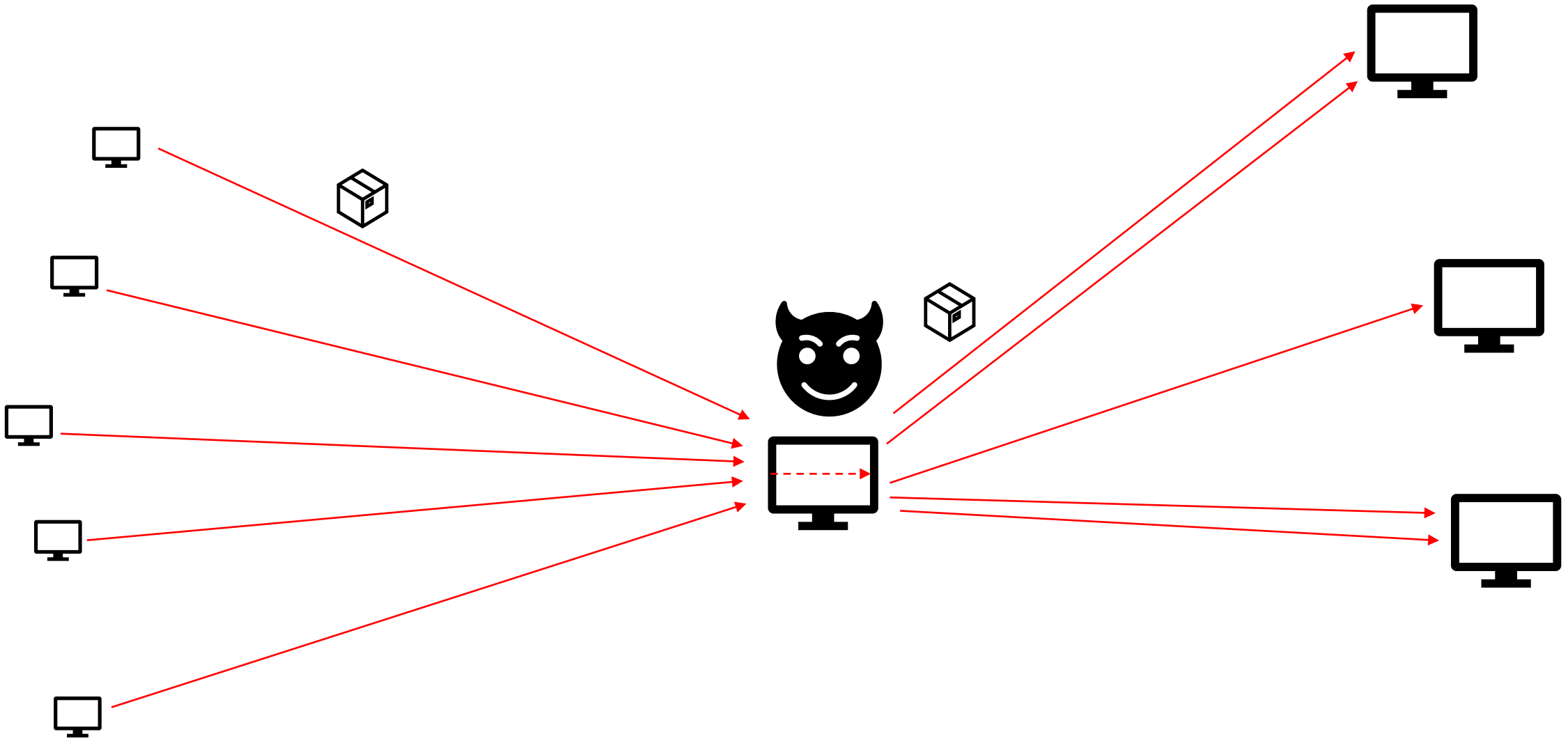
Classic stepping-stone problem



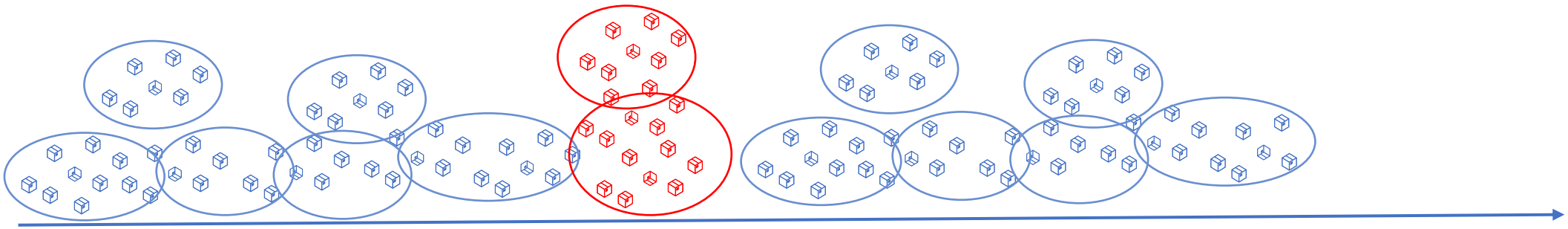
Classic stepping-stone problem



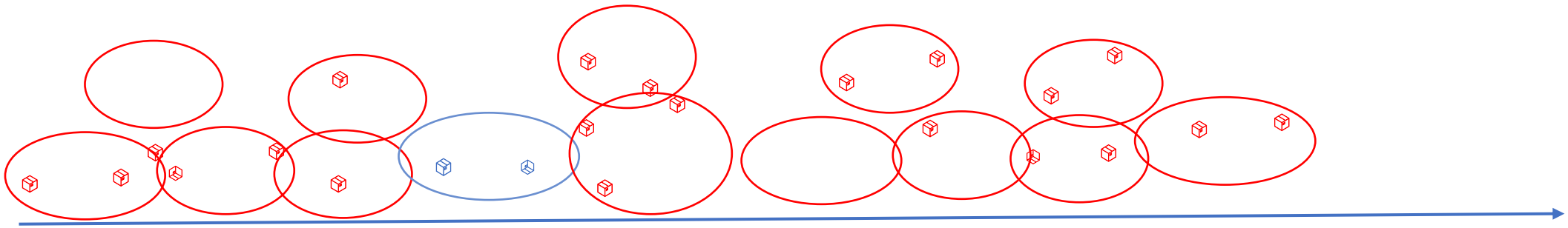
Our problem



Classic stepping-stone problem



Our problem



Import features

Classic stepping-stone

- Packet IATs
- Packet sizes
- Connection activity levels
- RTTs

Our problem (potentially)

- Ingoing/outgoing connection similarity over time
  - Similar port usage on both sides
  - Similar connection features (traffic rate,
  - Similar outgoing „response“ for incoming connections from different IPs

Current data and next steps

- Connections overall very similar
  - Similar sizes, duration, …
  - What‘s happening on port 3128?
  - Very constrained time-window

- Next steps:
  - Apply packet sampling to simulate „ISP view“
  - Connections need to be a bit more diverse to mimic different users