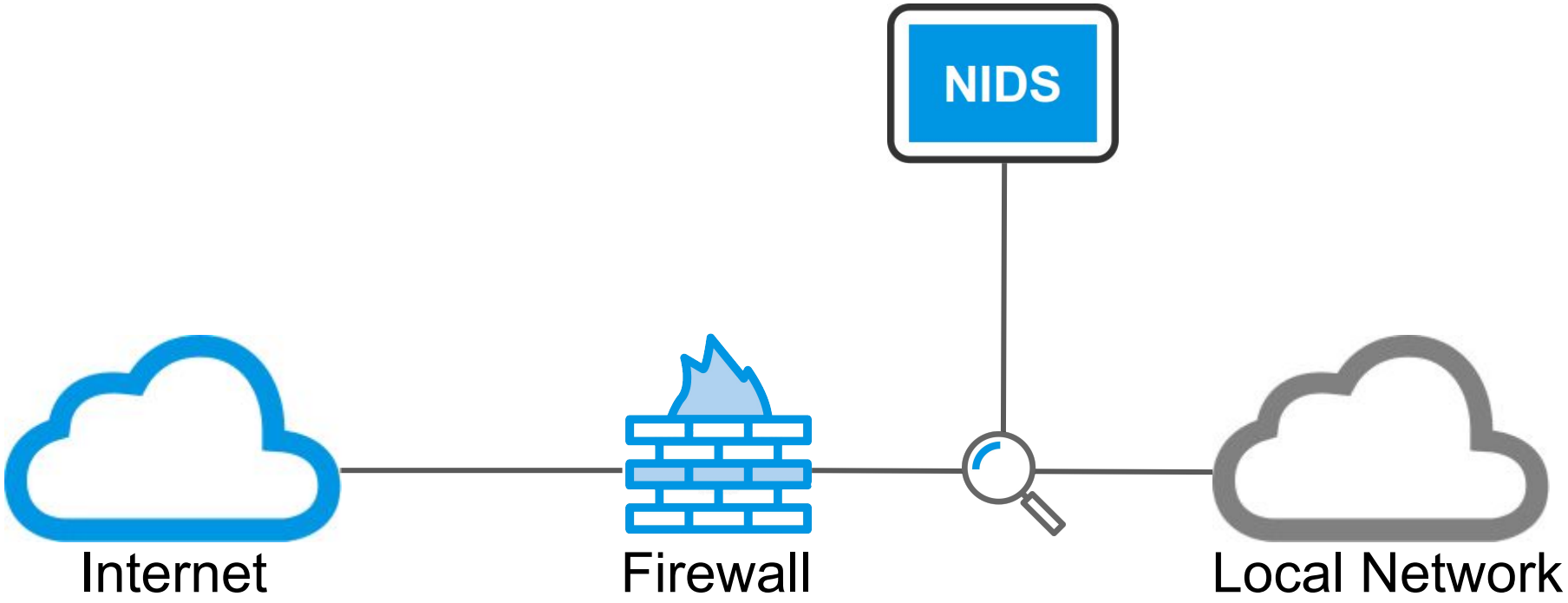
Syrius (**Sy**nthesis of Su**ri**cata R**u**le**s**)

Network Intrusion Detection Systems (NIDS)



Two main approaches

Anomaly based:

Can detect unknown attacks

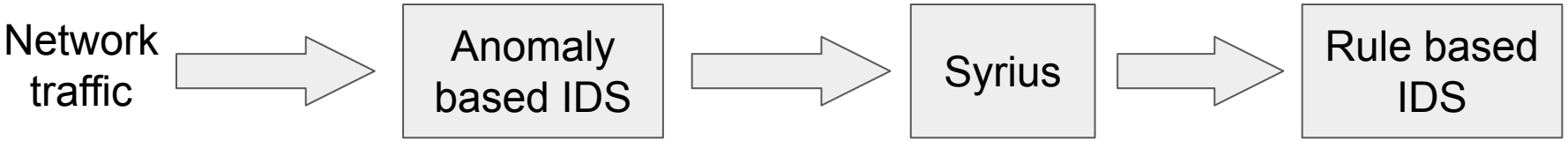
Higher rate of false alerts

Rule Based:

Precise for well known attacks

Creating rule sets can be time-consuming

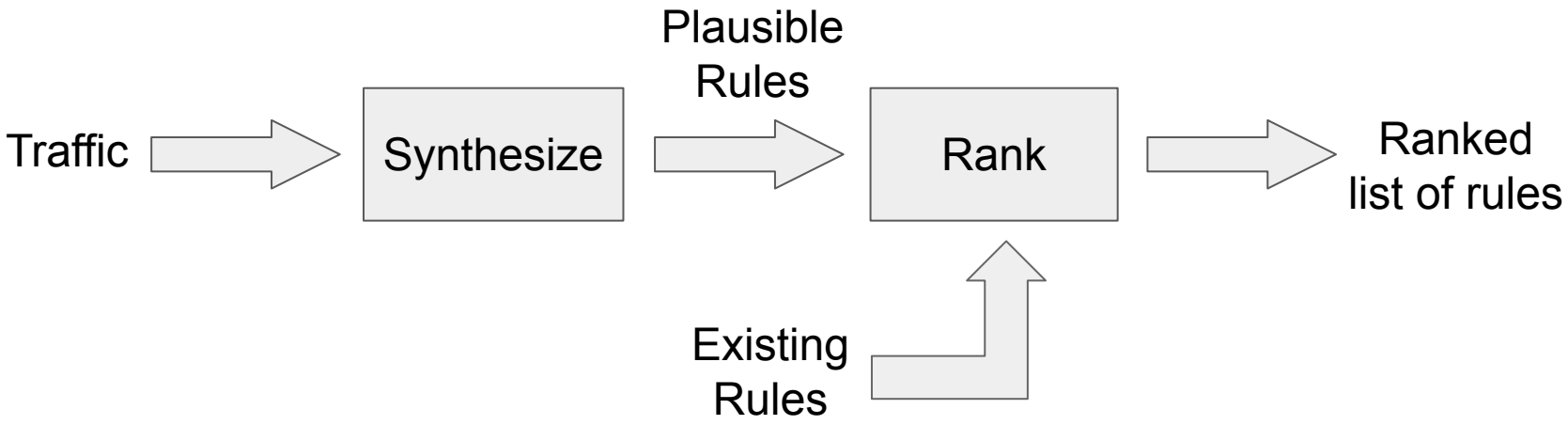
Our goal: Synthesize rules from traffic



Current status

- Generating a (huge) set of possible rules
- Sorting this set to get the best rules
    - Problem: The golden rule is far from the top of the sorted set

Syrius


Traffic
Synthesize
Plausible Rules
Rank
Ranked list of rules
Existing Rules

Synthesis