Protect Real-Time and Critical Industrial Automation Traffic with Firewall Optimizations

Prof. Dr. Tobias Heer – University of Esslingen

ESSLINGEN UNIVERSITY

1. Motivation

Firewalls filter traffic based on the **IP header of the packets** and the rules configured in the ruleset of the firewall. Each rule in the ruleset has five parameters (i.e., source and destination IP, source and destination port, and protocol).

Industrial control applications require all traffic to have a **static** time for transmission (aka **latency**) from sender to receiver. To protect the industrial applications, we want to place firewalls within the communication.

The **configuration** of the ruleset (e.g., order of rules) **influences the latency** of the firewall. Hence, industrial applications require specific focus on optimized firewall rulesets!

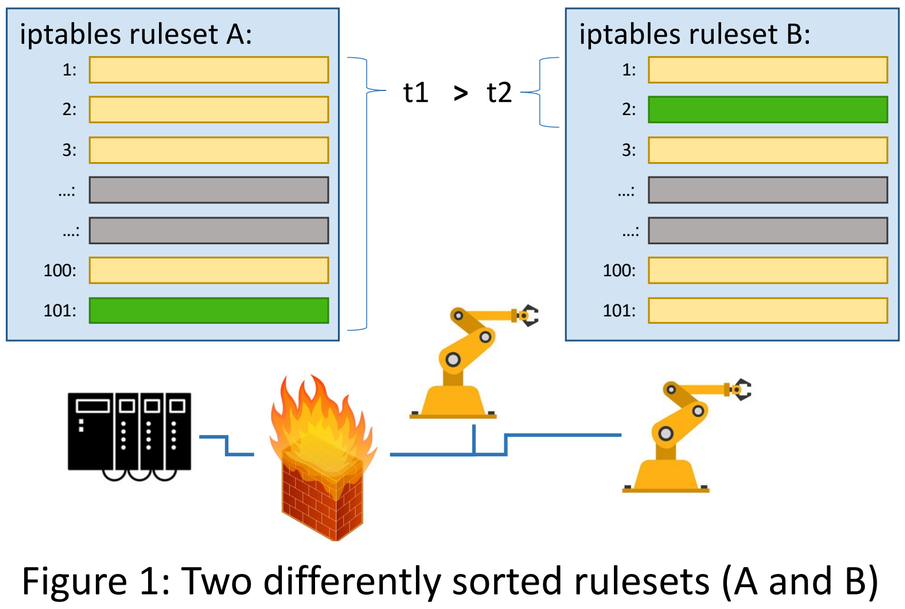
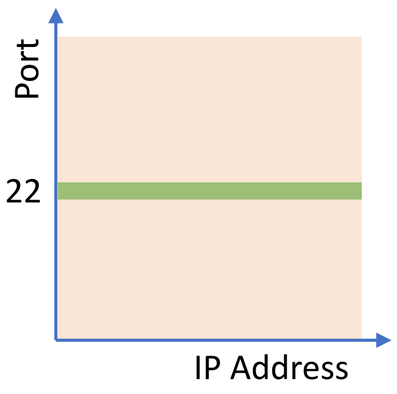


Figure 1: Two differently sorted rulesets (A and B) result in different latencies (t1 > t2)

2. Research Idea: Geometric Representation of Firewall Rules

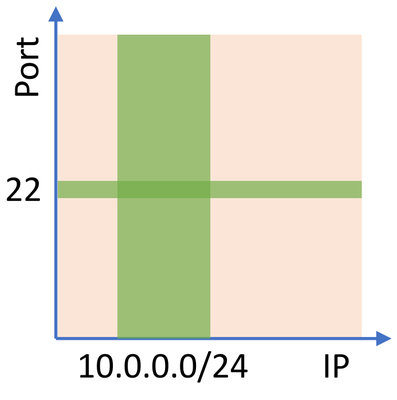
Firewall rules define a set of allowed packets. As firewall rules have five parameters, they define allowed packets within these five dimensions. In geometry, n-dimensional sets and overlaps of sets can be represented with the volume of geometric structures. Hence, we want to represent these rules in 5-dimensional structures.

1. What if a firewall would only have two parameters?



Single Rule

- In a 2D space, all packets allowed by one rule are marked in green (red background is disallow)
- Figure: A single rule allowing all packets with Port 22

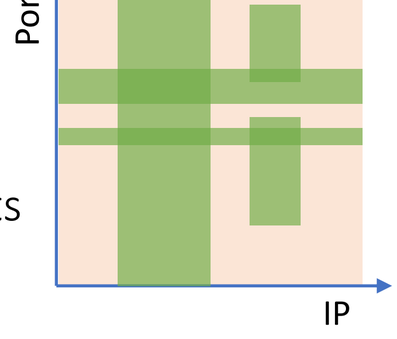


Two Rules

- Multiple rules can define overlays
- Figure: Additional rule allowing all traffic for network 10.0.0.0/24

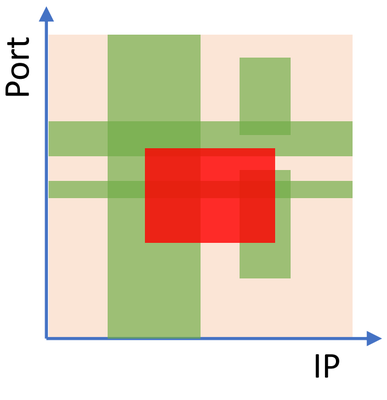
2. Let's add more rules!

- Combination of parameters and parameter ranges define smaller areas for allowed packets
- Green area presents allowed packets
- Structure gets more complex



3. Mixture of ACCEPT and DROP rules

- Defines additional holes in geometric representation (see red area in figure)
- Order of rules is crucial, as rules are applied from top to bottom



3. Goal and Structure of the Research Project

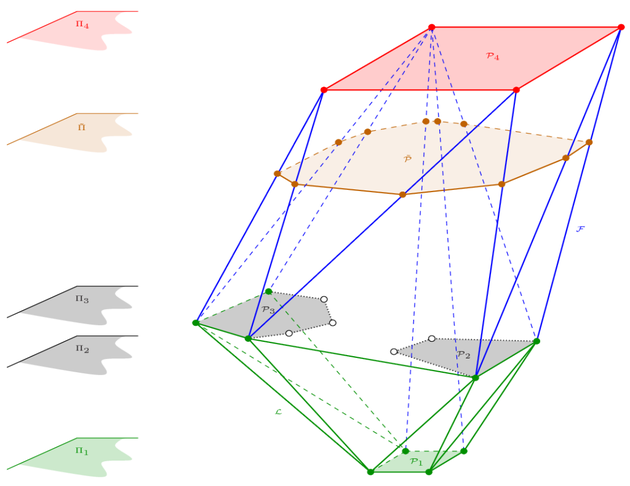


Figure 2: Representation of a four-dimensional convex polytope [1]

Goal: More than two parameters!

- A typical firewall rule has five parameters. i.e., source and destination IP, source and destination port, and protocol
- How to visualize more than three parameters? → Convex Polytopes
- Compare rulesets for equivalence!
- Can we optimize the rulesets to fulfill industrial requirements?

Semester One

- Transform firewall rulesets into convex polytope structures
  - Implementation in C, Python, or Java
- Implement state of the art comparison algorithms for convex polytopes

Semester Two

- Optimize firewall rulesets with the help of the convex polytope structure

4. References

[1] Karavelas, Menelaos I. and Tzanaki, Eleni. (2011). Convex hulls of spheres and convex hulls of convex polytopes lying on parallel hyperplanes.

Supervisors: Prof. Dr. Tobias Heer, Lukas Bechtel, Markus Schramm and Nils Lohmiller
{tobias.heer, lukas.Bechtel, markus.schramm, nils.lohmiller}@hs-esslingen.de

If you have any questions, get in touch with us!