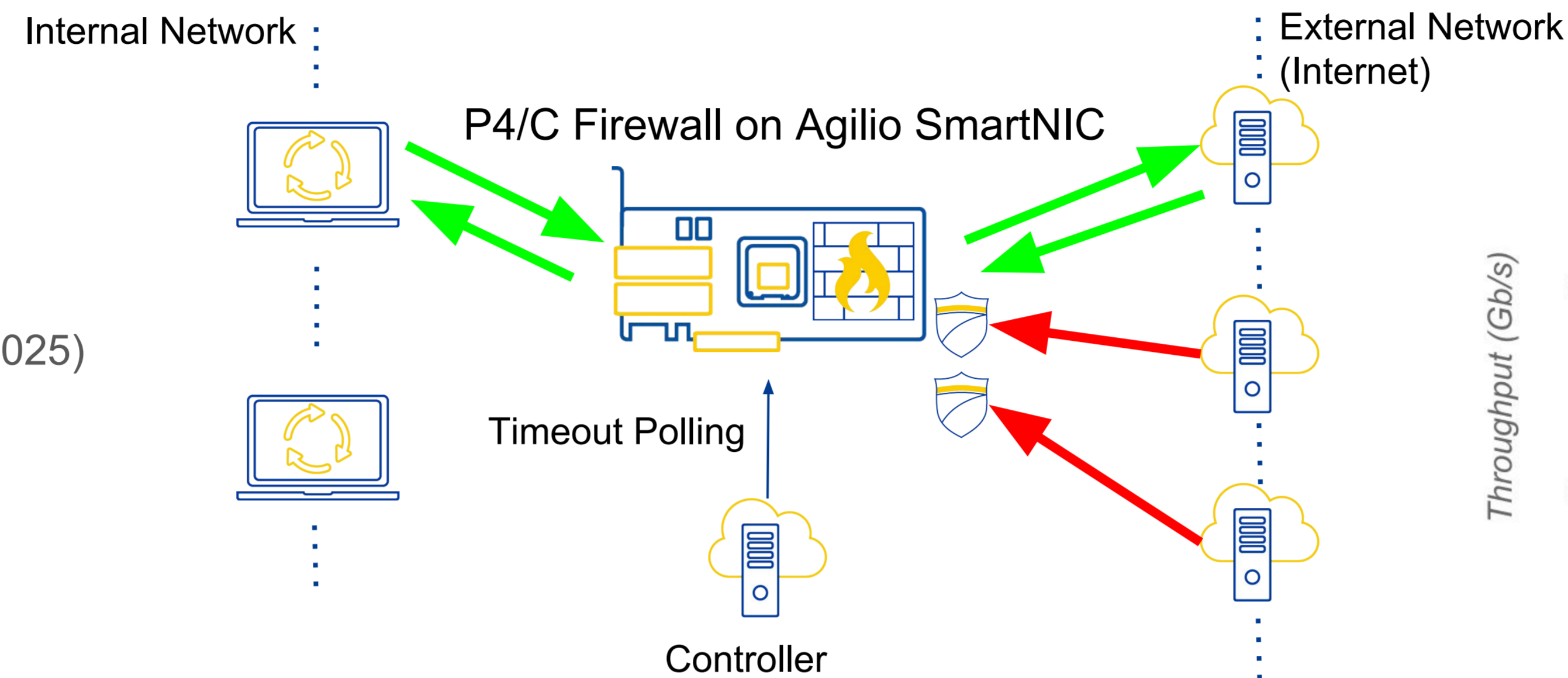


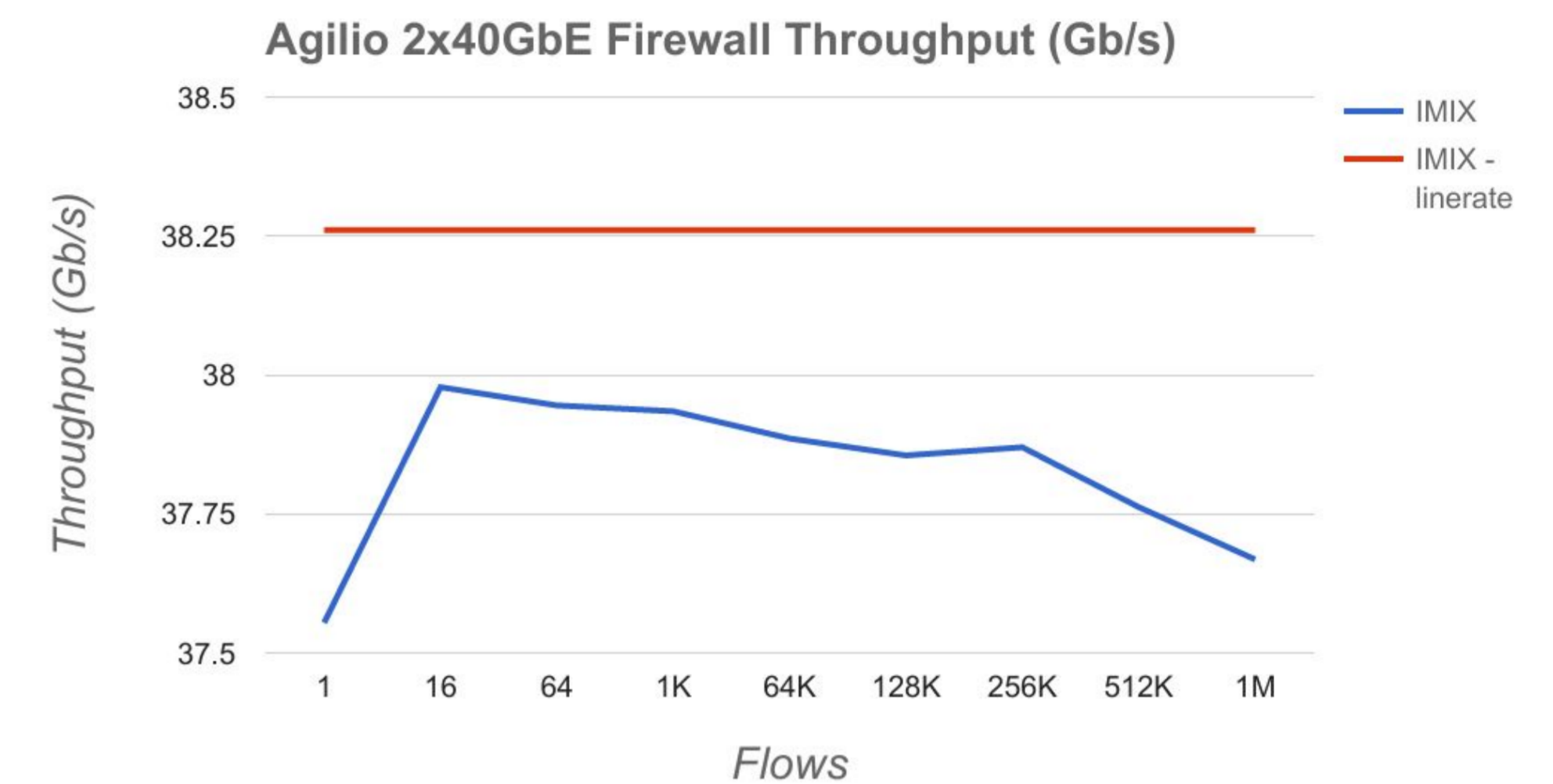
P4/C Stateful Firewall

NAT

- Network Address Translation
- Internal -> External -> Hit
 - Translate Source IP and Port
 - Source IP -> Public IP
 - Source Port -> Port Selected (starting at 1025)
- External -> Internal -> Hit
 - Translate Destination IP and Port
 - Destination IP -> Stored Private IP
 - Destination Port -> Stored Private Port



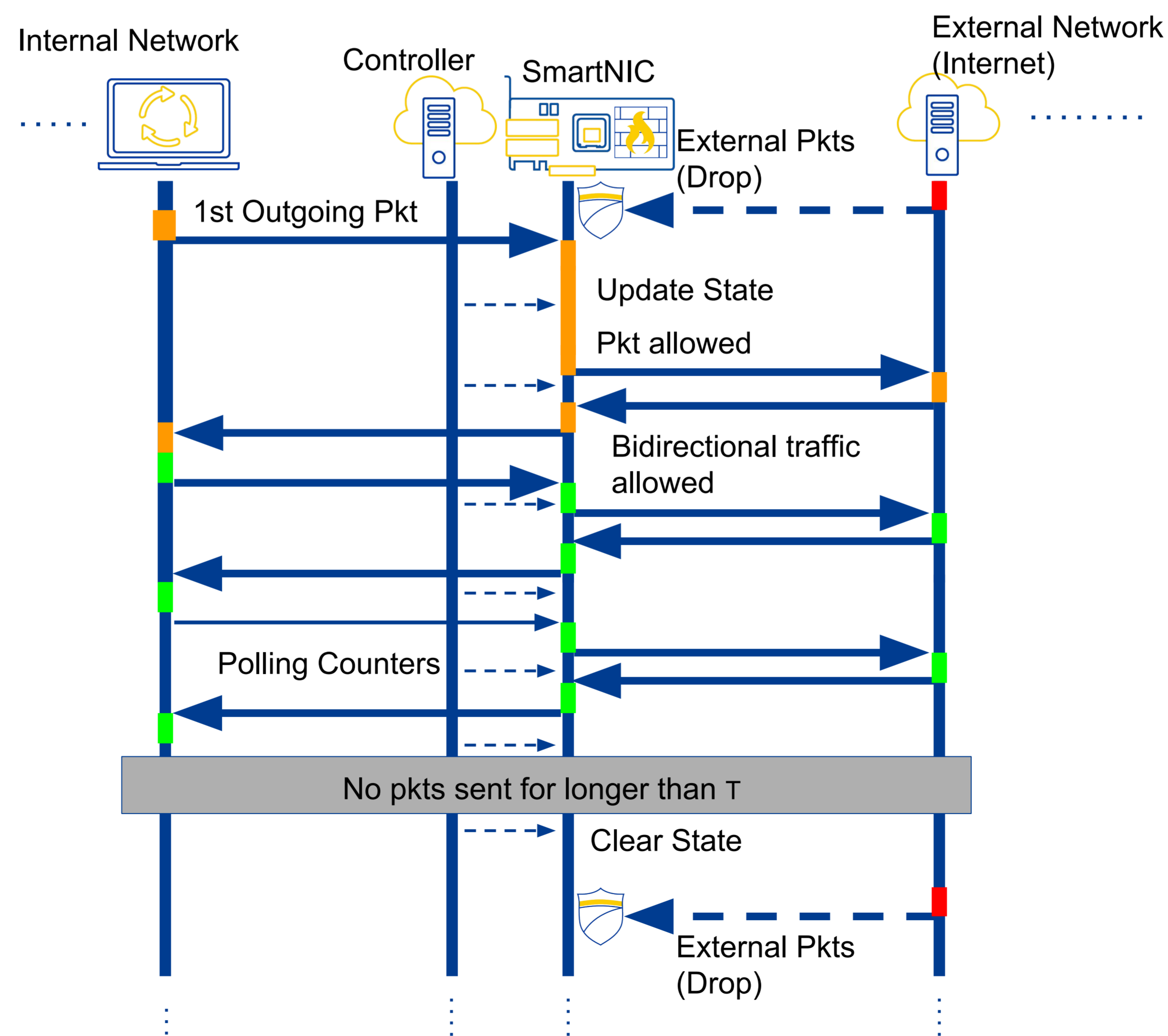
Performance



P4 Application

● P4 Tables, Actions and Rules

- Lookup State Table
 - Match - Ingress Port
 - Action - Apply hash function for state lookup
- NAT Table
 - Match - State, Ingress Port
 - Actions
 - Int_ext_hit
 - Forward to External Network
 - Ext_int_hit
 - Forward to Internal Network
 - Int_ext_miss
 - Forward to External Network
 - Flag to update state
 - Ext_int_miss
 - drop
- Update State
 - Match - State, Egress Spec
 - Action - Update State
- Controller Packet Table
 - Match - Ingress Port
 - Action - Clear Ports Timeouts



https://github.com/open-nfpsw/p4c_firewall

Sandbox C

● State Table

- Hashtable - Separate Chaining Linked List
 - Hash Key
 - State for P4 rule
 - Public/Private IP for NAT
 - Public/Private Port for NAT
 - Hit Count
 - Hit Count Comparison for Timeouts

● Bitfield

- Public Ports Used/Available per IP
 - Accessed by all MEs and Threads
 - Atomic memory operations needed to keep it reliable
- Public Port: 1025 1026 1027 ... 1032 1033 1034 ... 65535
- 001110111000....
- In Use Timed Out In Use Available