Cybersecurity (Security+) and P4 Programmable Switches

Lab 10: Limiting the Impact of SYN Flood by Probabilistically Dropping Packets

Ali AlSabeh, Jorge Crichigno
University of South Carolina
http://ce.sc.edu/cyberinfra

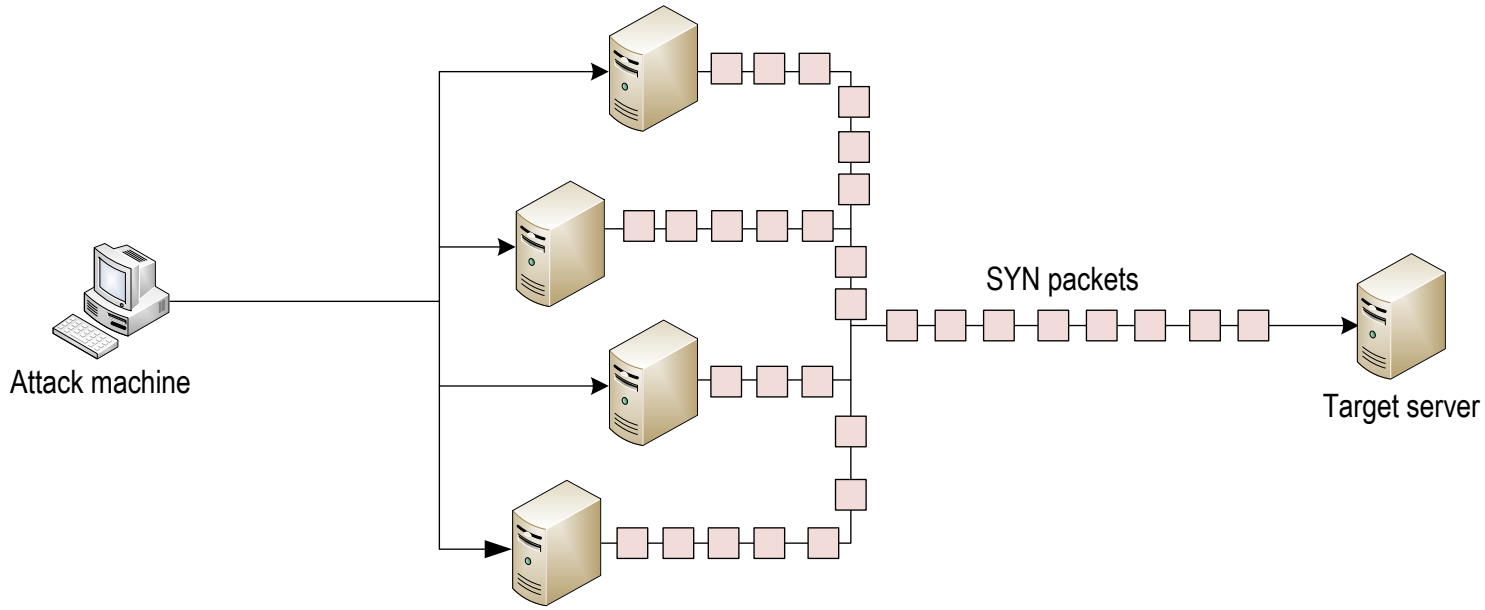
Western Academy Support and Training Center (WASTC)
University of South Carolina (USC)
Energy Sciences Network (ESnet)

June 23rd, 2023

Lab 10: Limiting the Impact of SYN Flood by Probabilistically Dropping Packets

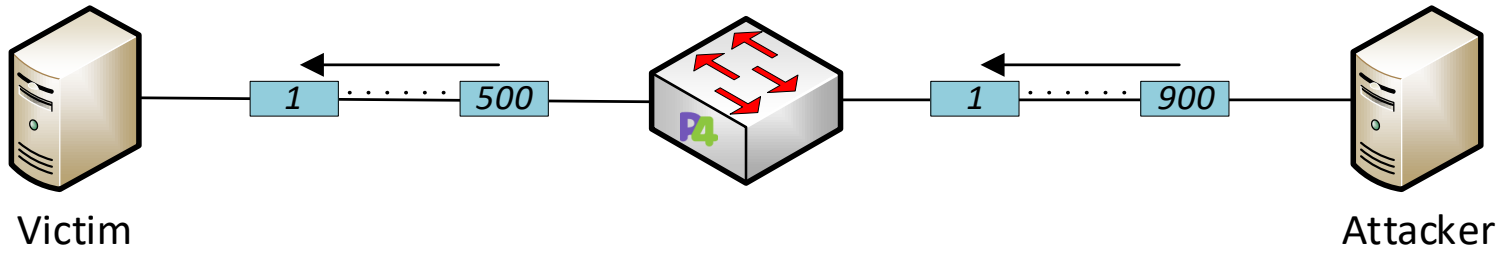
SYN Flood Attack

- Massive amount of TCP SYN requests with spoofed IP addresses are sent to the server
- These connections consume the server's resources, making it unresponsive to legitimate traffic
- Server start "half-open" connections
- Connections build up until queue is full and all additional requests are blocked



Attack Scenario

- Count the number of SYN packets per second in the data plane
- When the count exceeds a predefined threshold, the switch starts dropping SYN packets
- The dropping percentage is configured by the administrator from the control plane

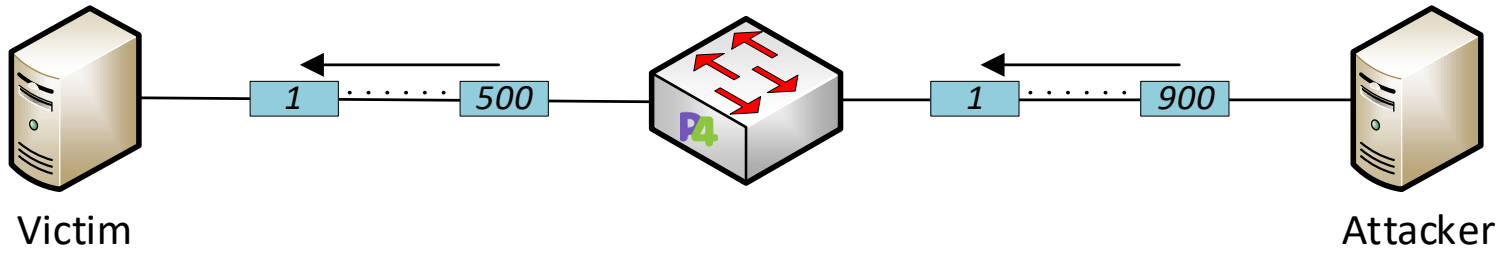


SYN packets threshold: 100

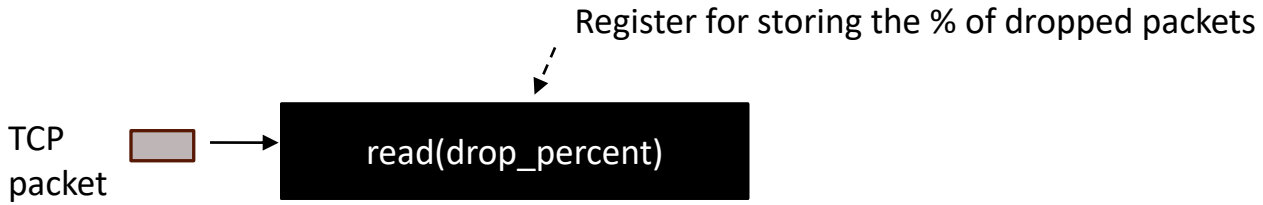
Dropping percentage: 50%

Attack Scenario

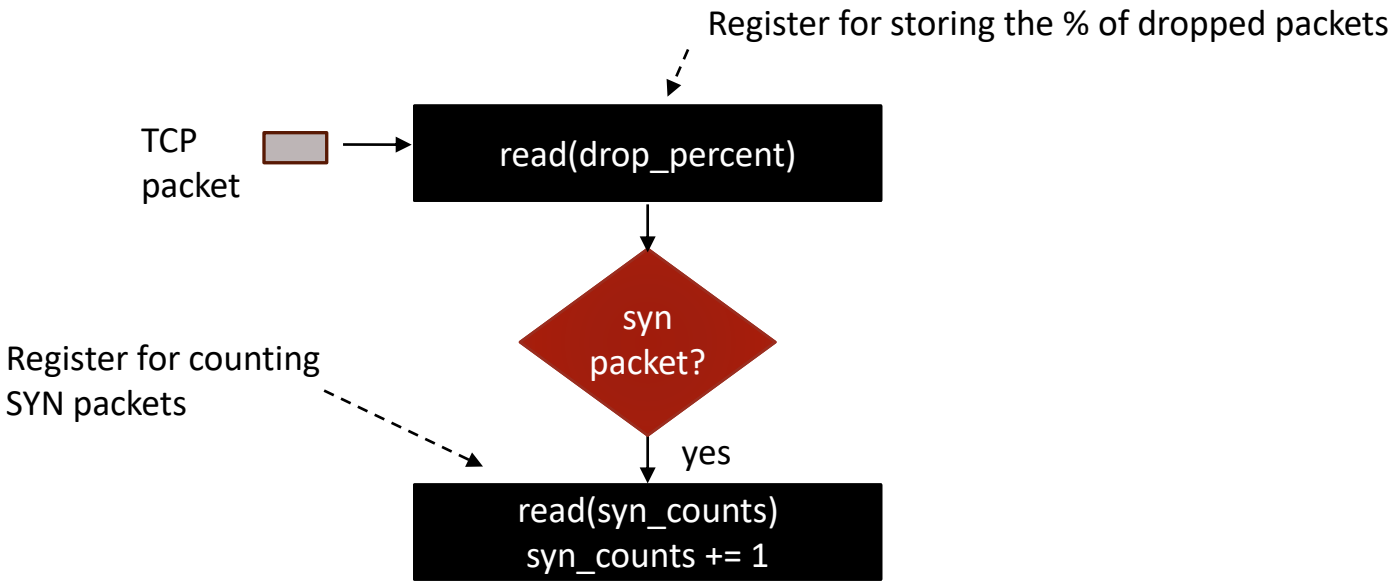
- Assuming that the attacker is generating 900 SYN packets per second
- The SYN count detection threshold is 100 packets per second
- Assume that the drop percentage is 50%
- The number of packets that will be forwarded is:
  - $100 + (900 - 100) * 50/100 = 100 + 800/2 = 500$



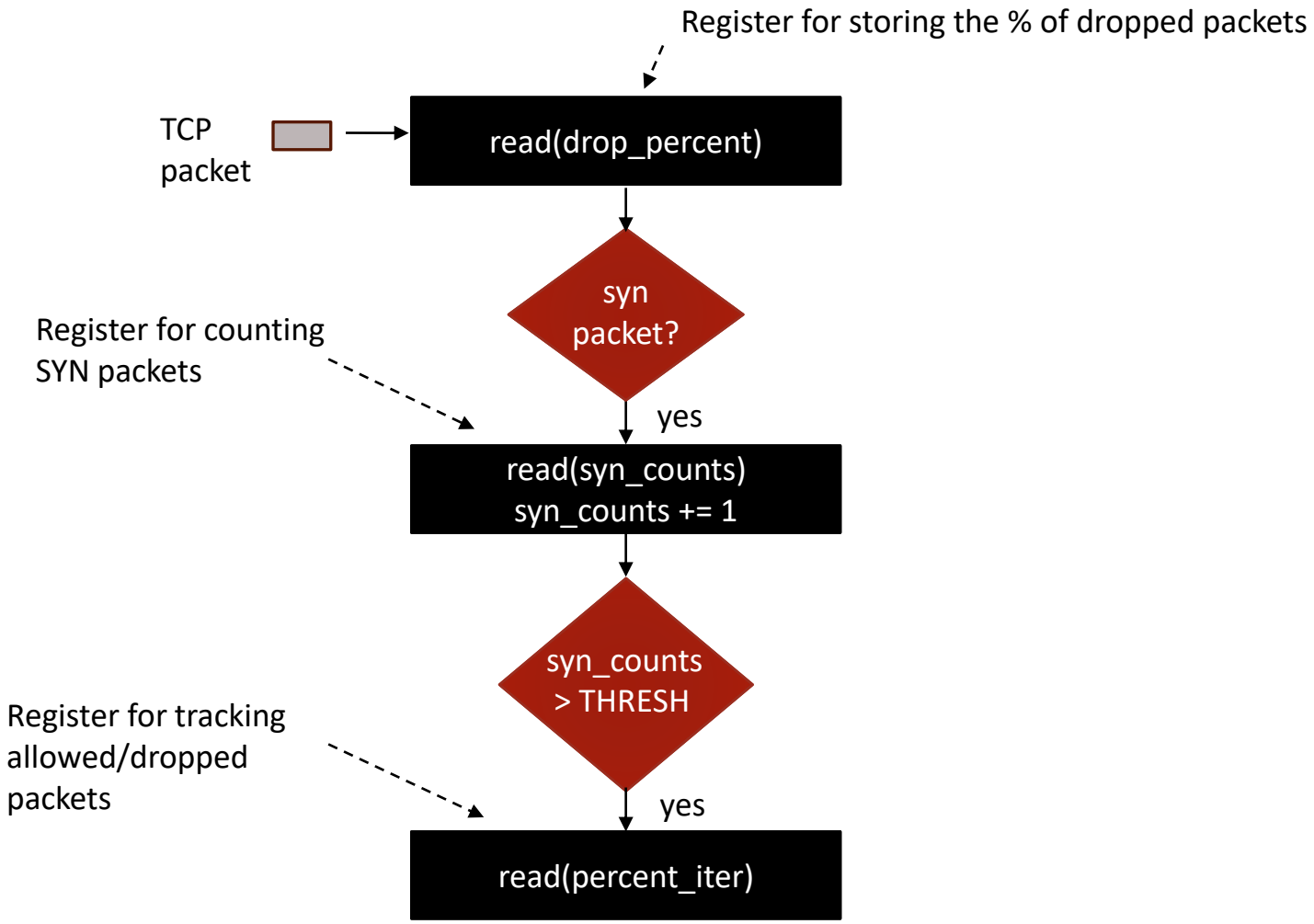
Flow of the SYN Flood Detection in P4



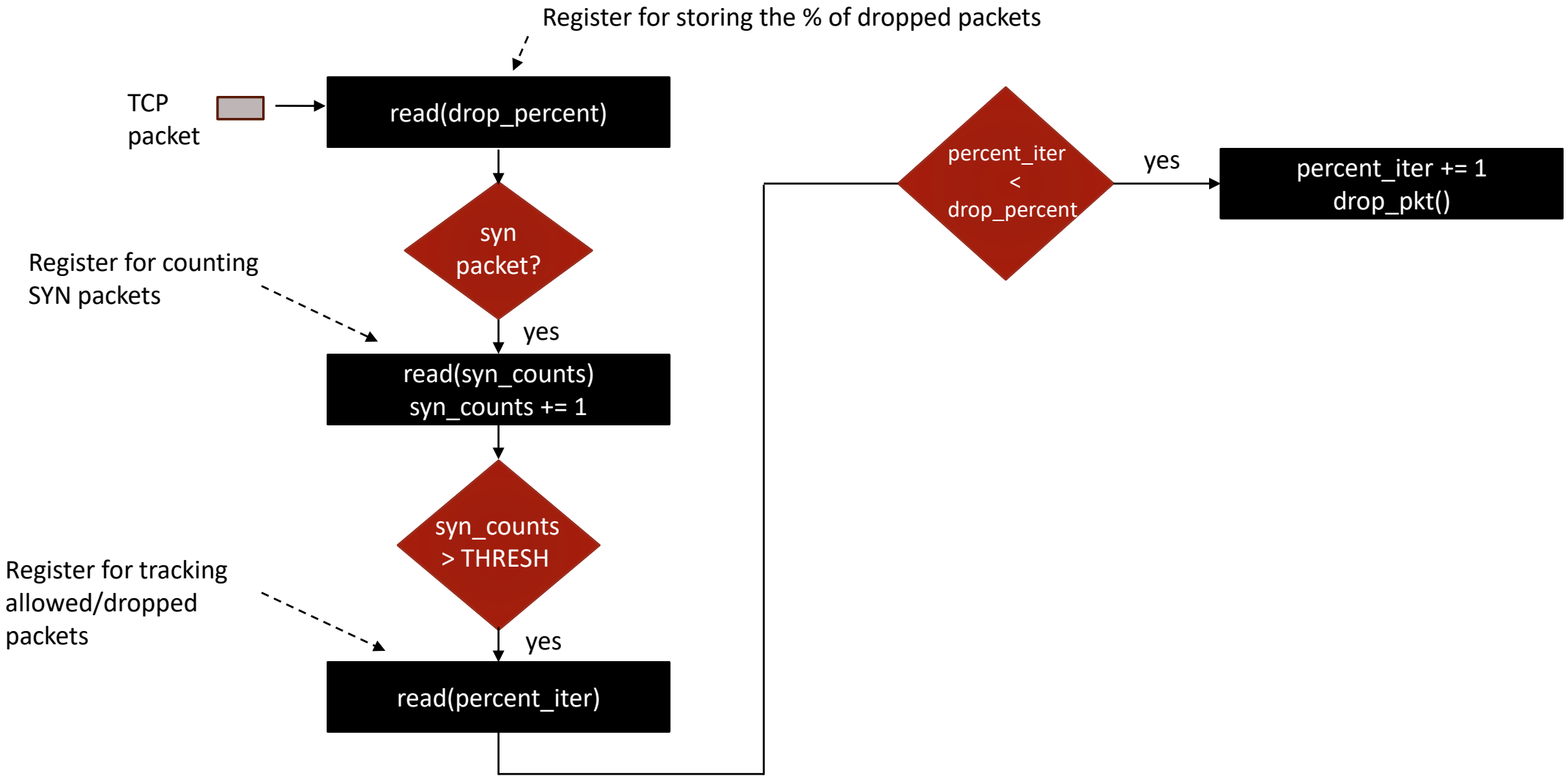
Flow of the SYN Flood Detection in P4



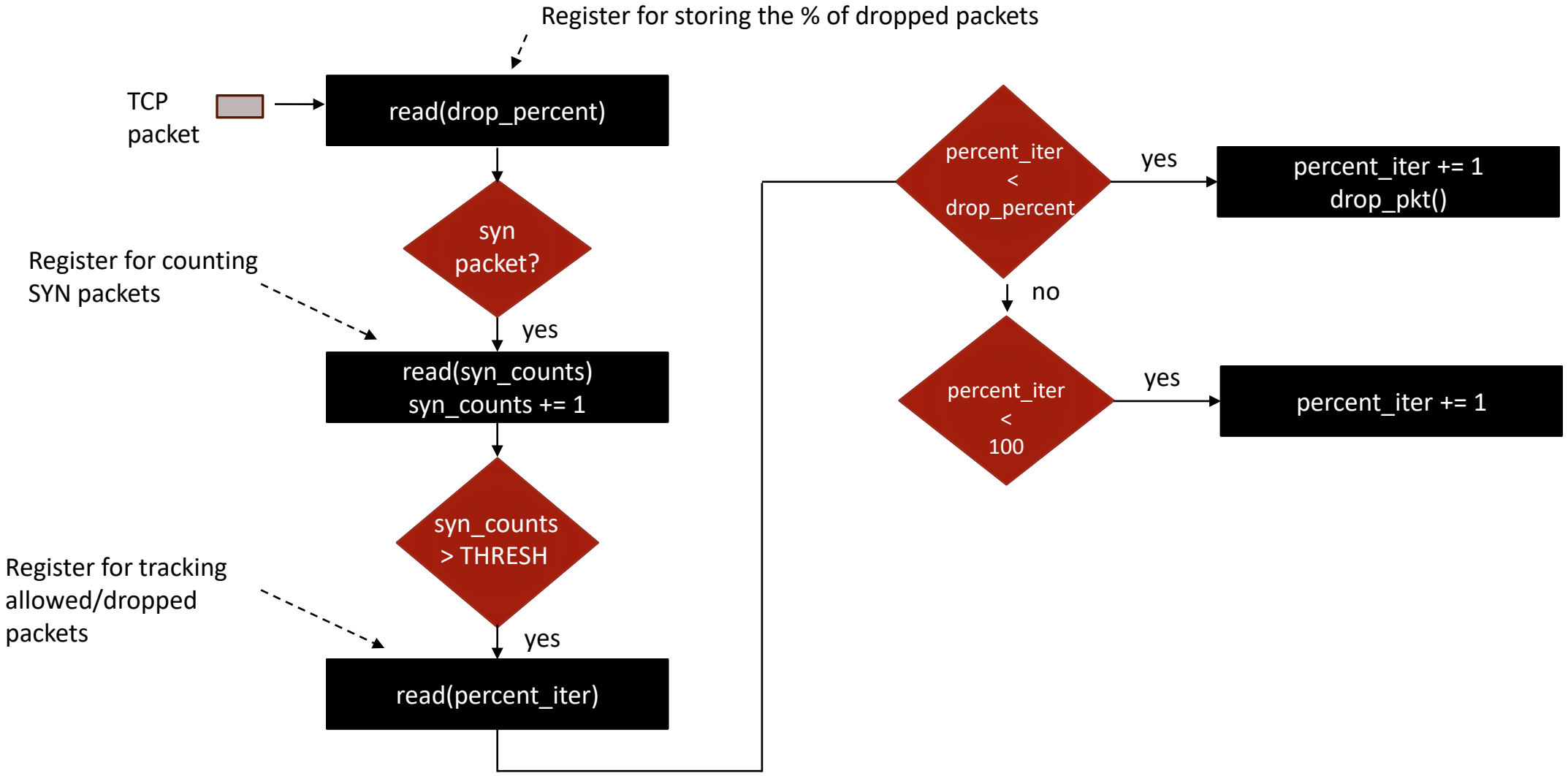
Flow of the SYN Flood Detection in P4



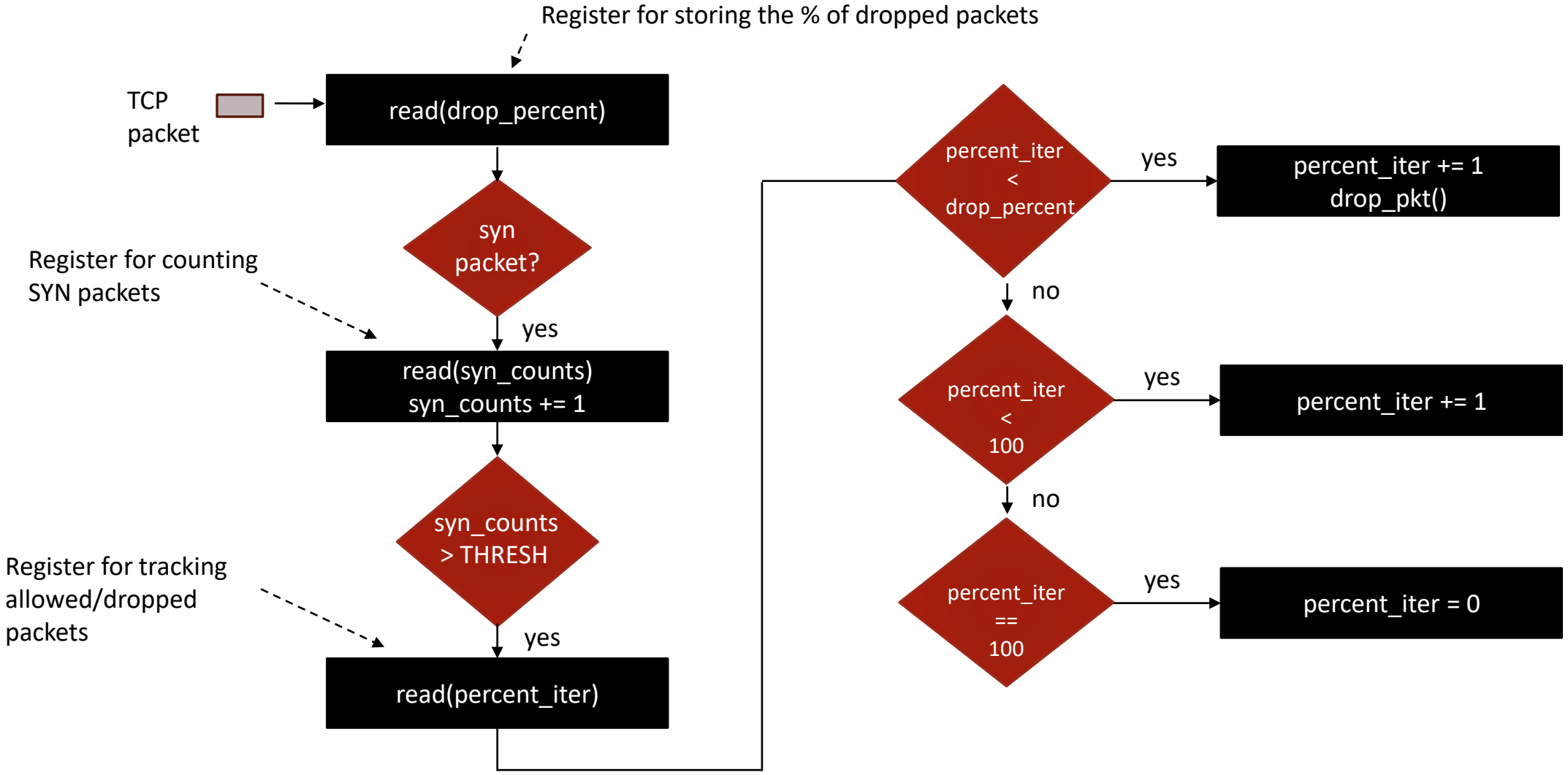
Flow of the SYN Flood Detection in P4



Flow of the SYN Flood Detection in P4

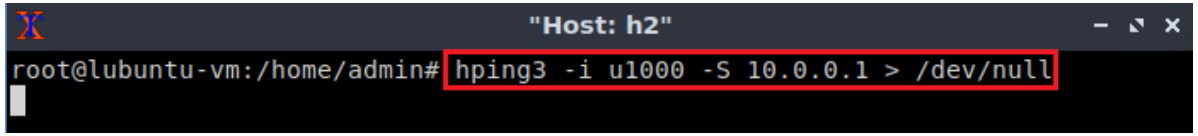


Flow of the SYN Flood Detection in P4

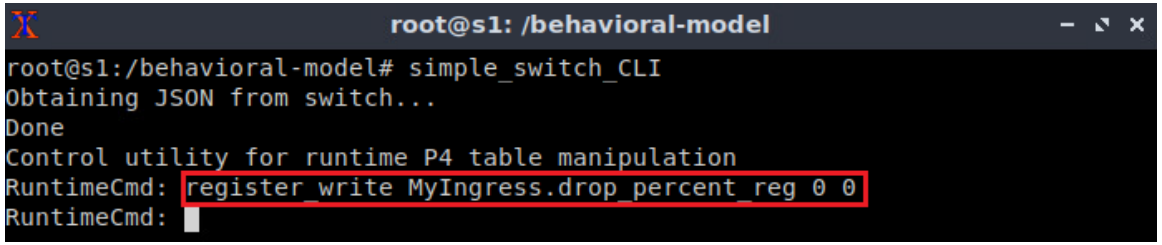


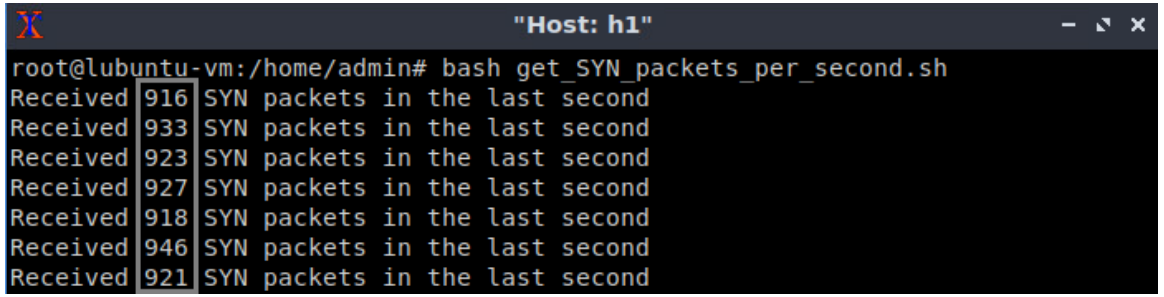
SYN Flood Detection in P4

Perform SYN flood attack



No SYN flood mitigation in P4





SYN flood mitigation in P4 (50% packet drop)