



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>

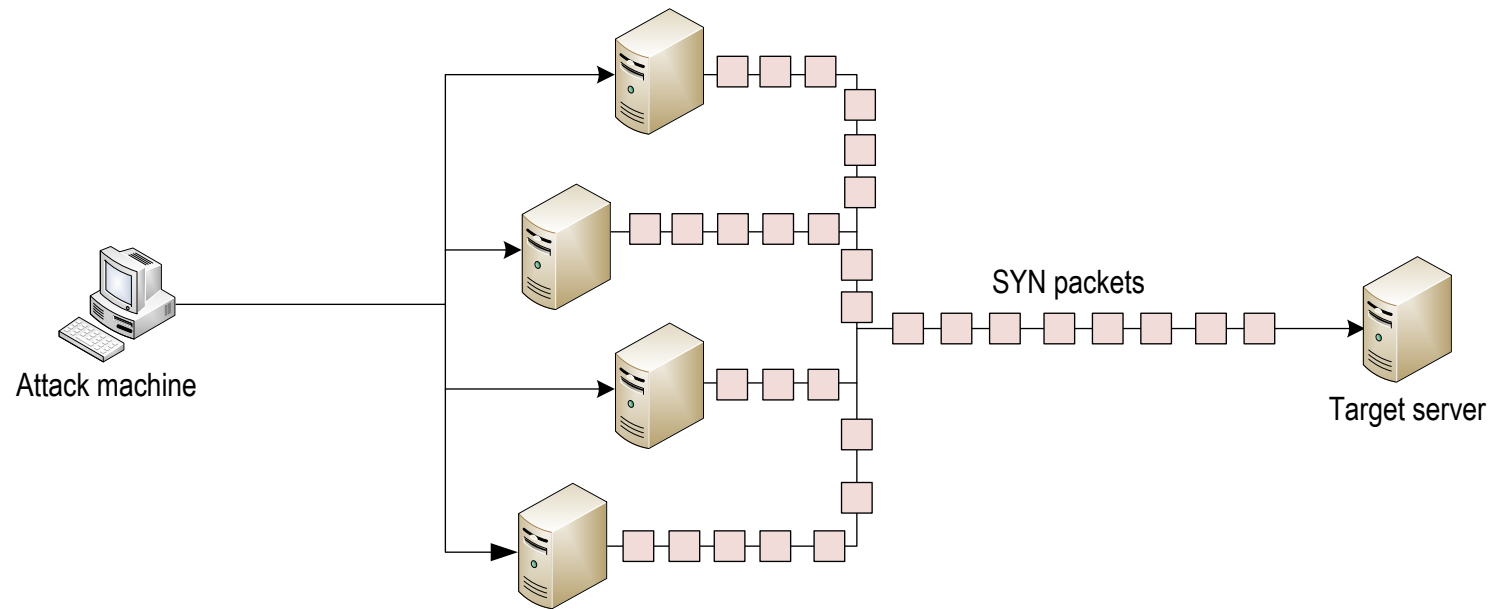
Western Academy Support and Training Center (WASTC)
University of South Carolina (USC)
Energy Sciences Network (ESnet)

June 23rd, 2023

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

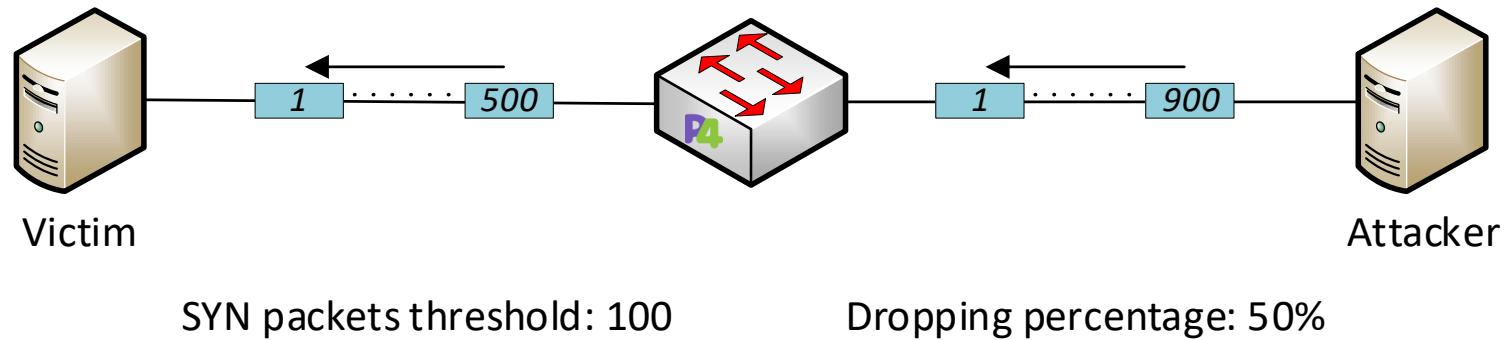
SYN Flood Attack

- 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



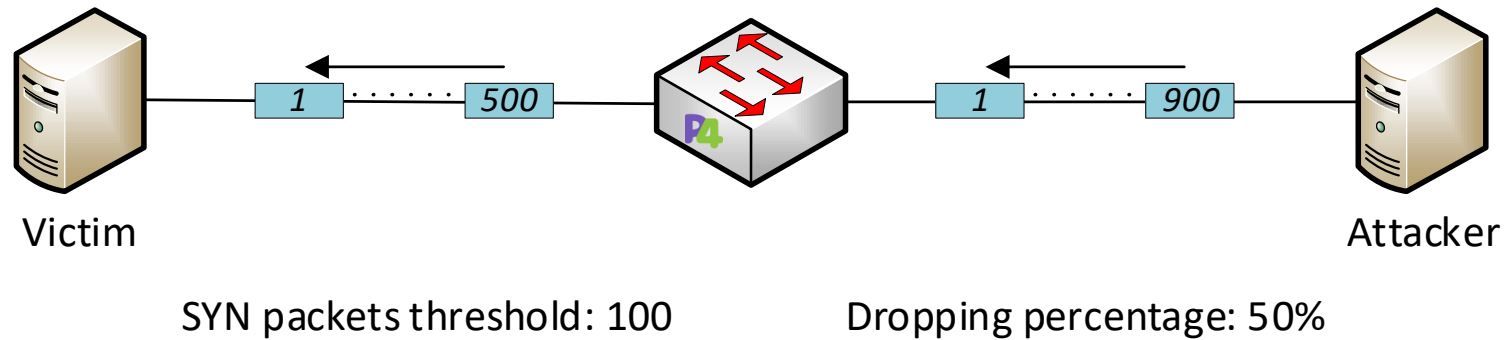
Attack Scenario

- 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

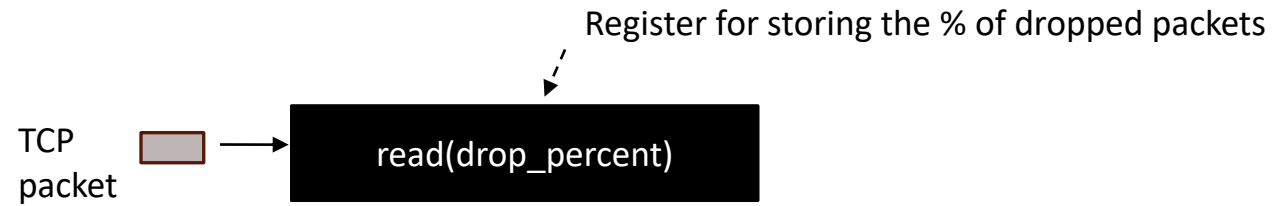


Attack Scenario

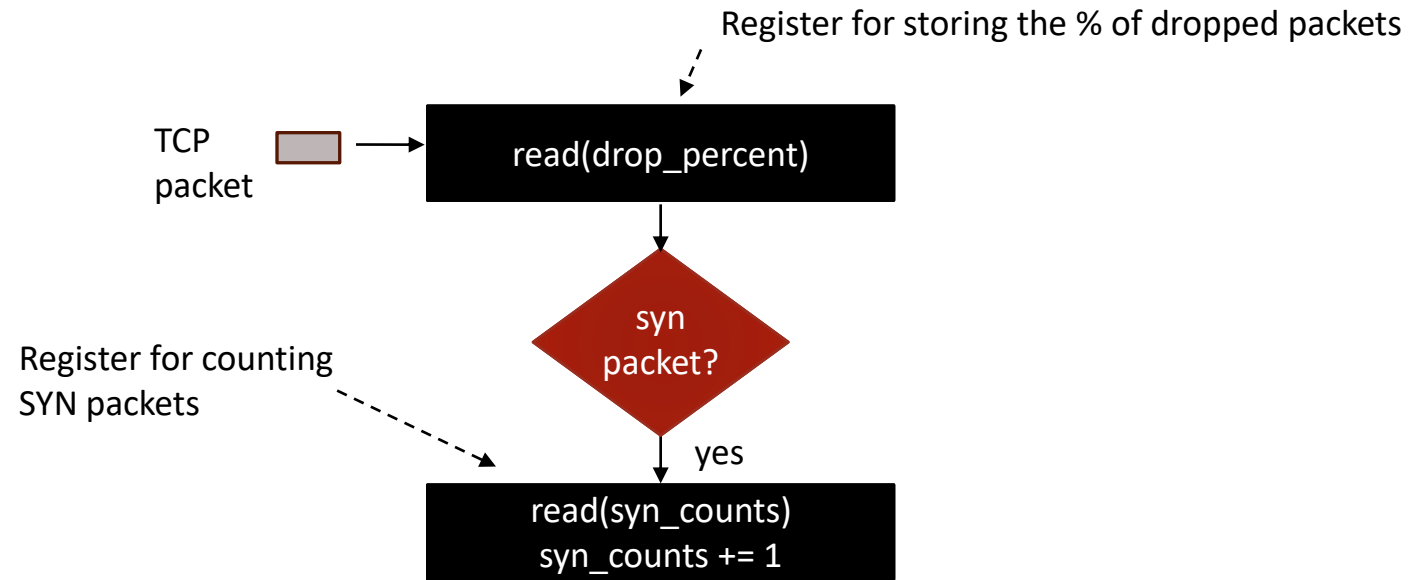
- Assuming that the attacker is generating 900 SYN packets per second
- The SYN count detection threshold is 100 packets per second
- Assume that the drop percentage is 50%
- The number of packets that will be forwarded is:
 - $100 + (900 - 100) * 50/100 = 100 + 800/2 = 500$



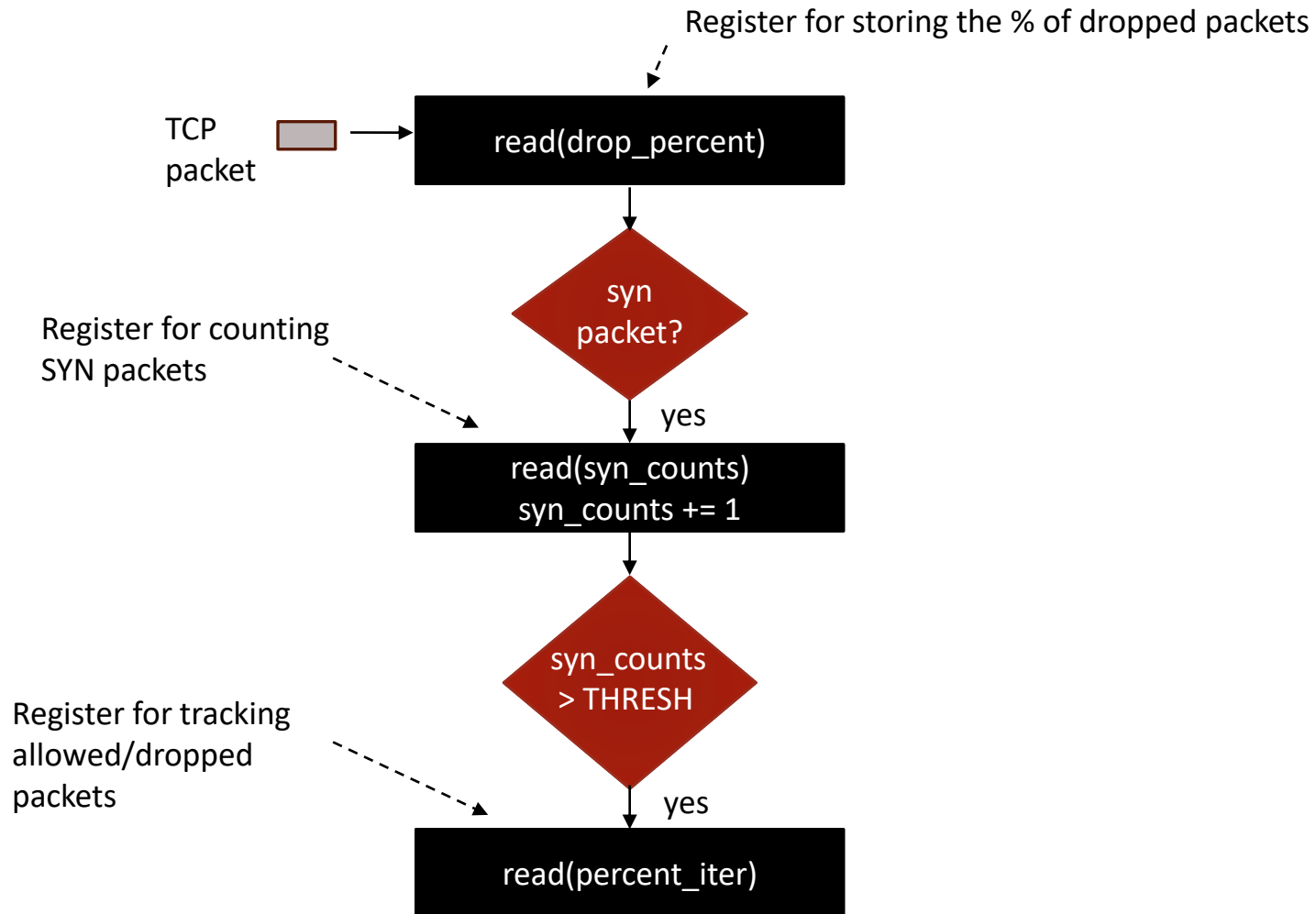
Flow of the SYN Flood Detection in P4



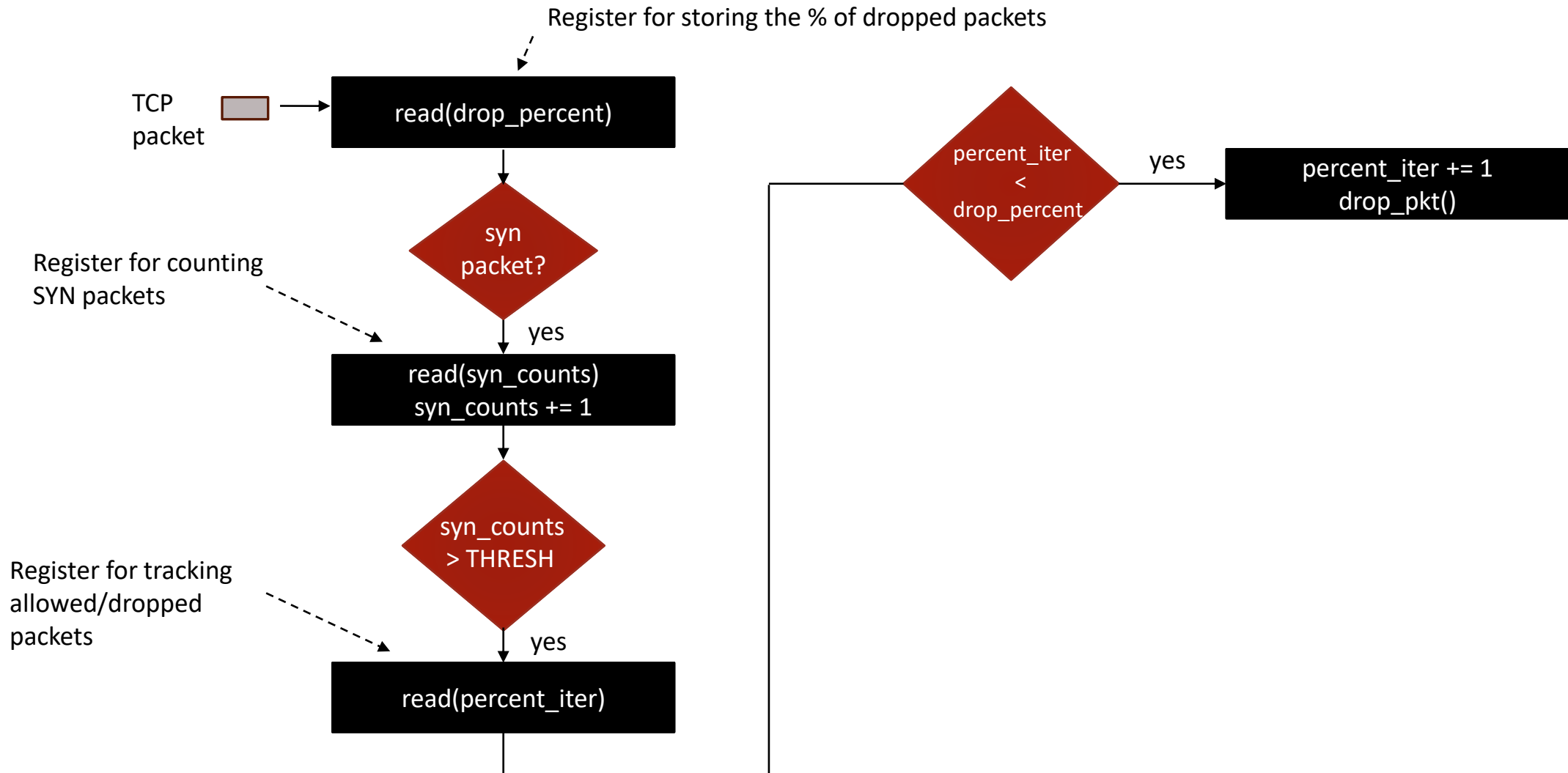
Flow of the SYN Flood Detection in P4



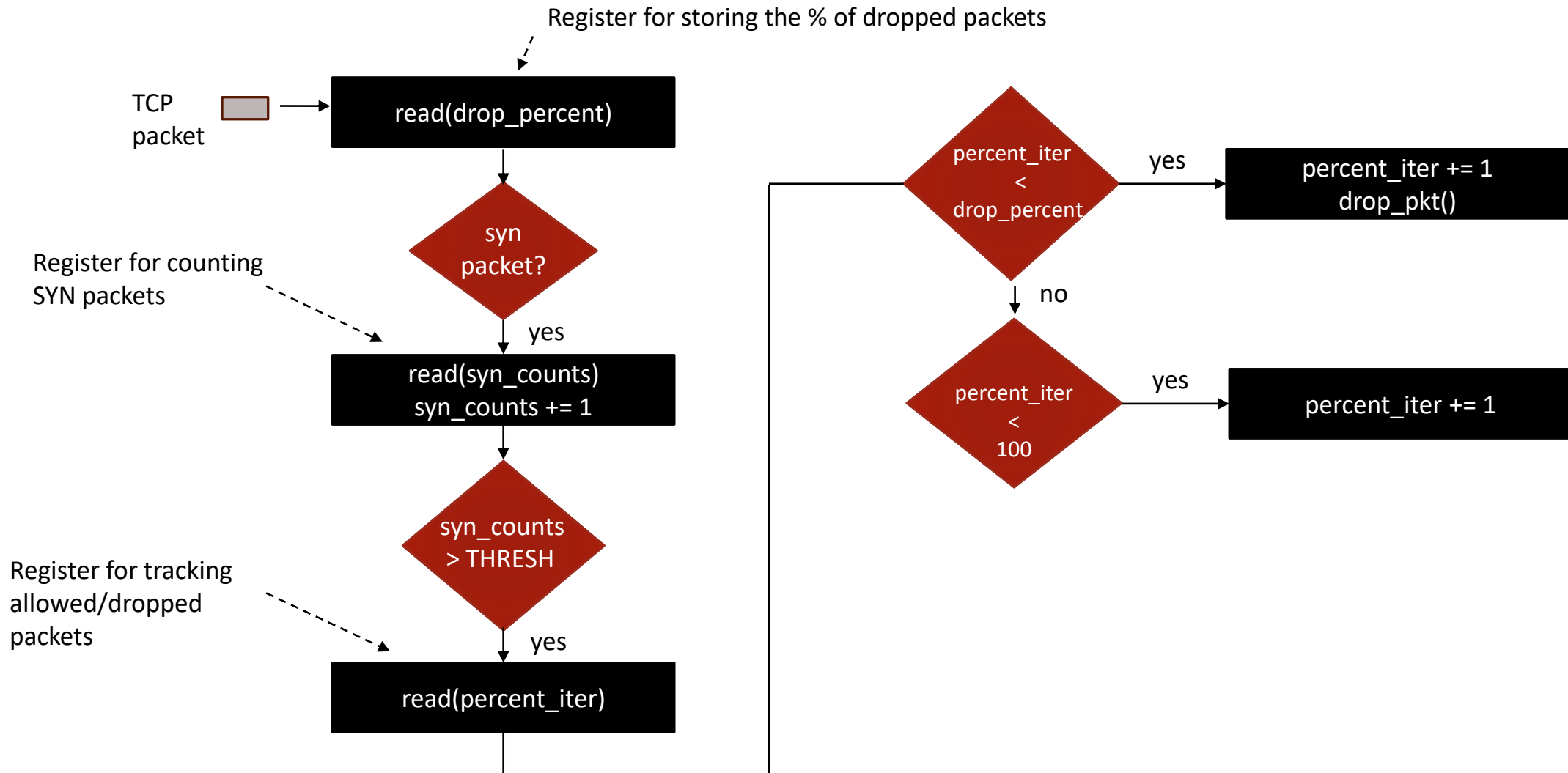
Flow of the SYN Flood Detection in P4



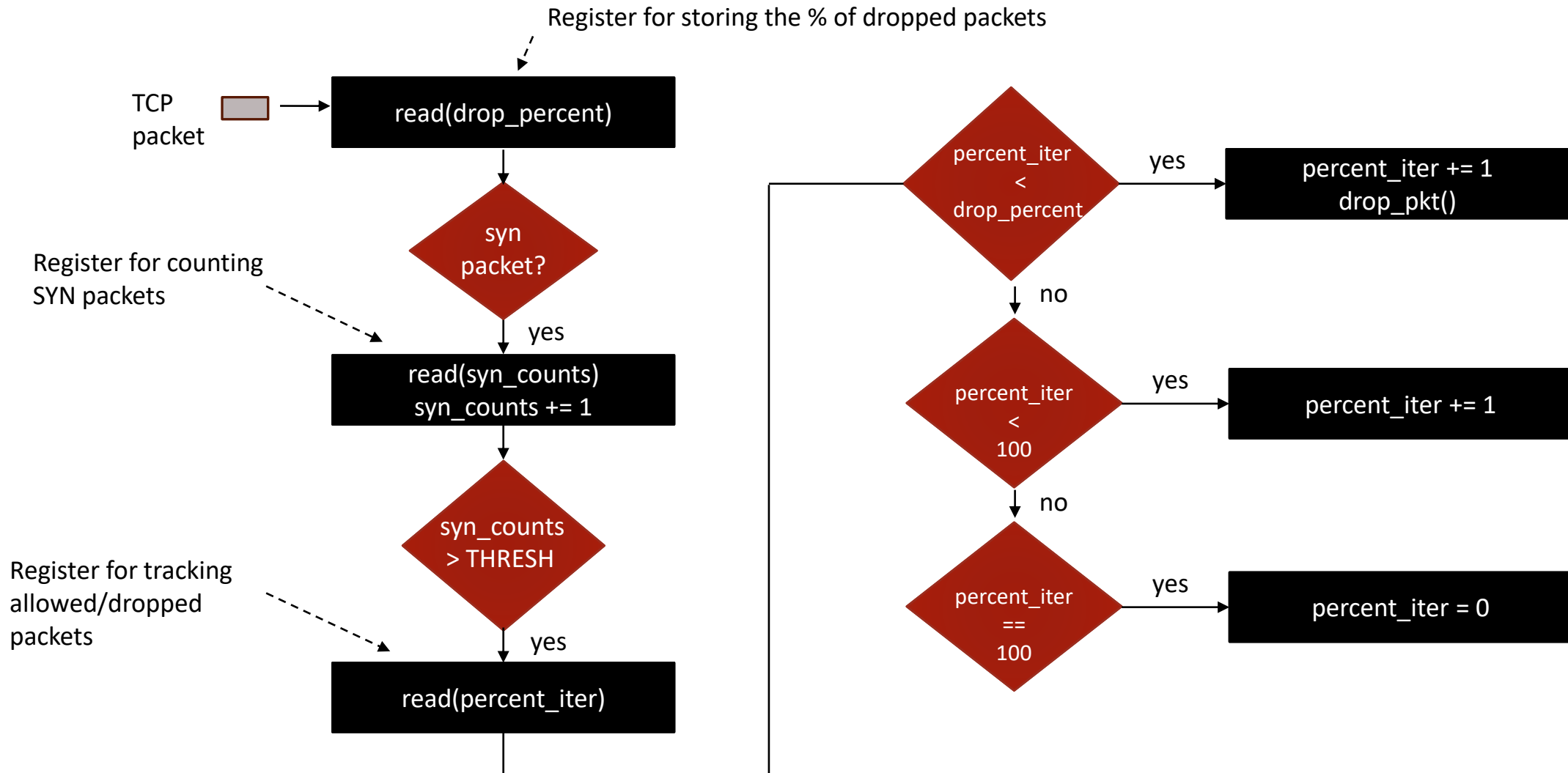
Flow of the SYN Flood Detection in P4



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

```
"Host: h2"  
root@lubuntu-vm:/home/admin# hping3 -i u1000 -S 10.0.0.1 > /dev/null
```

No SYN flood mitigation in P4

```
root@s1: /behavioral-model  
root@s1:/behavioral-model# simple_switch_CLI  
Obtaining JSON from switch...  
Done  
Control utility for runtime P4 table manipulation  
RuntimeCmd: register_write MyIngress.drop_percent_reg 0 0  
RuntimeCmd:
```

```
"Host: h1"  
root@lubuntu-vm:/home/admin# bash get_SYN_packets_per_second.sh  
Received 916 SYN packets in the last second  
Received 933 SYN packets in the last second  
Received 923 SYN packets in the last second  
Received 927 SYN packets in the last second  
Received 918 SYN packets in the last second  
Received 946 SYN packets in the last second  
Received 921 SYN packets in the last second
```

SYN flood mitigation in P4 (50% packet drop)

```
root@s1: /behavioral-model  
root@s1:/behavioral-model# simple_switch_CLI  
Obtaining JSON from switch...  
Done  
Control utility for runtime P4 table manipulation  
RuntimeCmd: register write MyIngress.drop percent reg 0 0  
RuntimeCmd: register write MyIngress.drop percent reg 0 50  
RuntimeCmd:
```

```
"Host: h1"  
Received 508 SYN packets in the last second  
Received 474 SYN packets in the last second  
Received 513 SYN packets in the last second  
Received 486 SYN packets in the last second  
Received 508 SYN packets in the last second  
Received 517 SYN packets in the last second  
Received 512 SYN packets in the last second  
Received 508 SYN packets in the last second
```