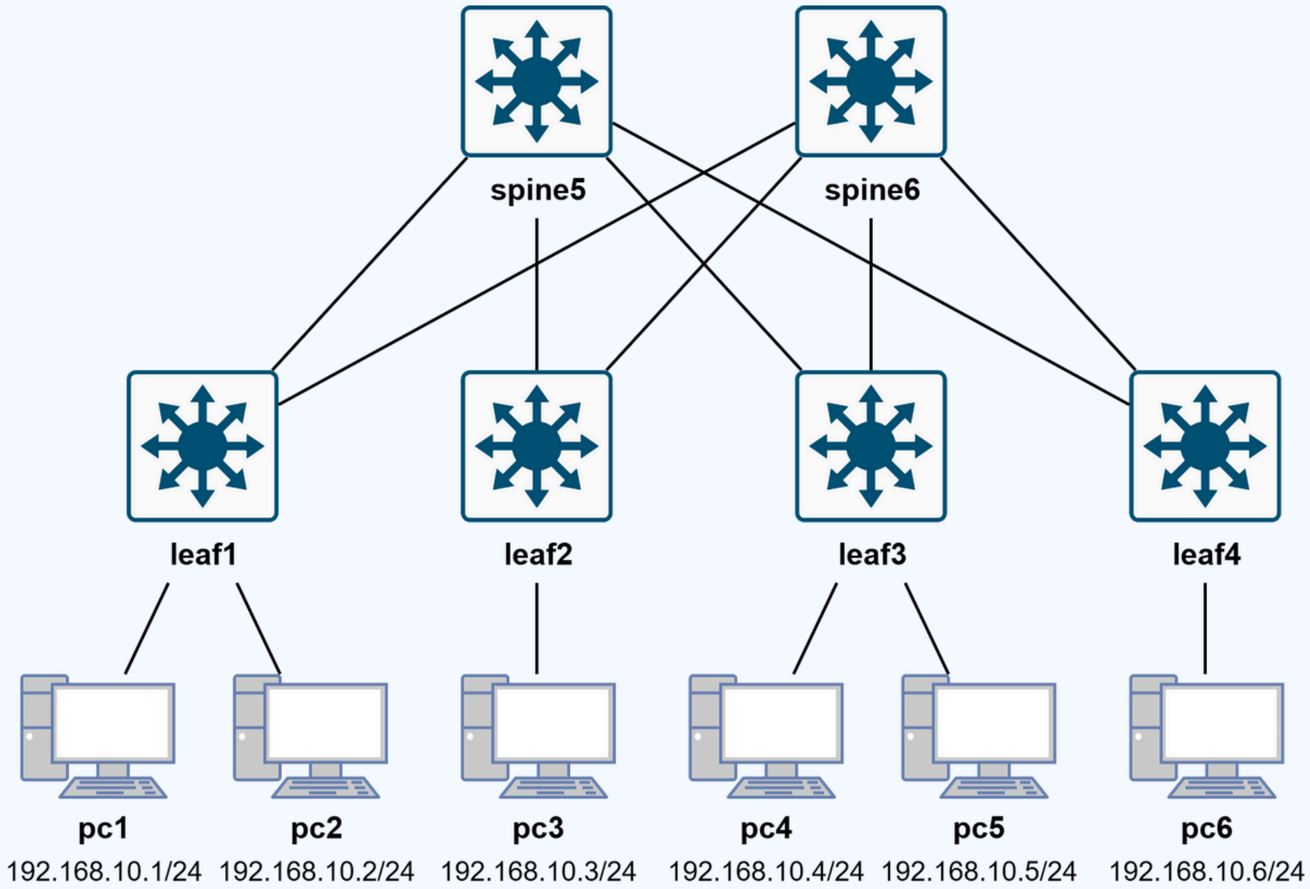
SDN REACTIVE FIREWALL:
DOS DETECTION & MITIGATION

Konrad Całka, Filip Kaczmarczyk, Konrad Maciejewski, Zuzanna Szuba

Sieci Sterowane Programowo, 22.01.2026

TOPOLOGIA


spine5
spine6
leaf1
leaf2
leaf3
leaf4
pc1
192.168.10.1/24
pc2
192.168.10.2/24
pc3
192.168.10.3/24
pc4
192.168.10.4/24
pc5
192.168.10.5/24
pc6
192.168.10.6/24

NARZĘDZIA

- Oracle VM VirtualBox
- Linux Ubuntu 22.04
- Python 3.9.19
- Mininet 2.3.1b4
- Ryu Controllerr 4.34
- Snort 2.9.15.1
- hping3
- iperf

GENERATORY RUCHU

RUCH NORMALNY

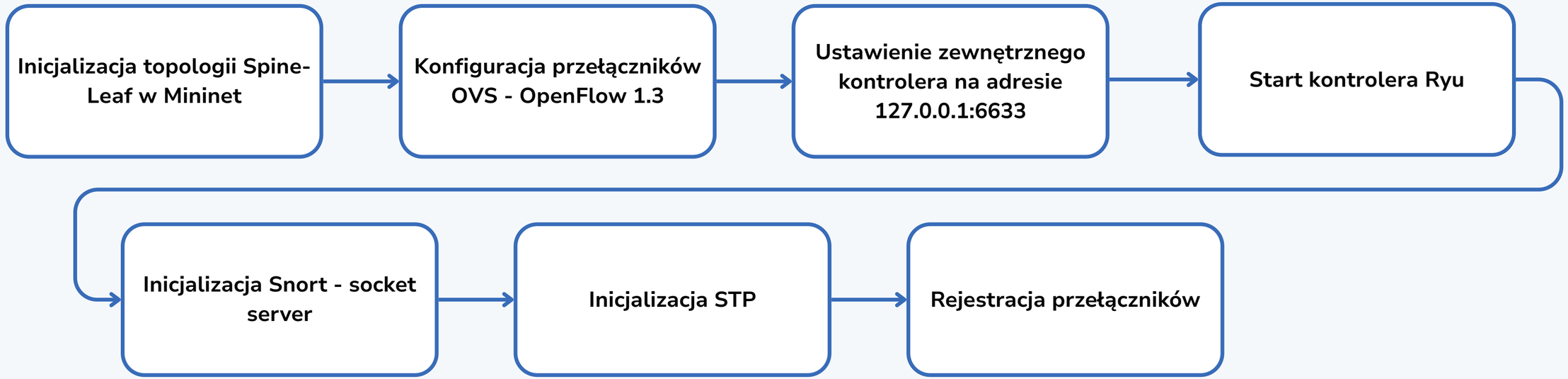
- **iPerf**
- serwer: pc3
- klienci: pc1, pc2, pc4, pc5
- transmisja równoległa
- różne czasy trwania
- losowe opóźnienia rozpoczęcia transmisji

FAZA ATAKU

- **hping3**
- pc1 uruchamia normalny ruch do pc3 na 120 s
- pc6 atakuje pc3 zalewając sieć wiadomościami TCP SYN wysyłanymi na port 5001 przez 60 s
- w rezultacie na pc1 pojawia się gwałtowny spadek przepustowości

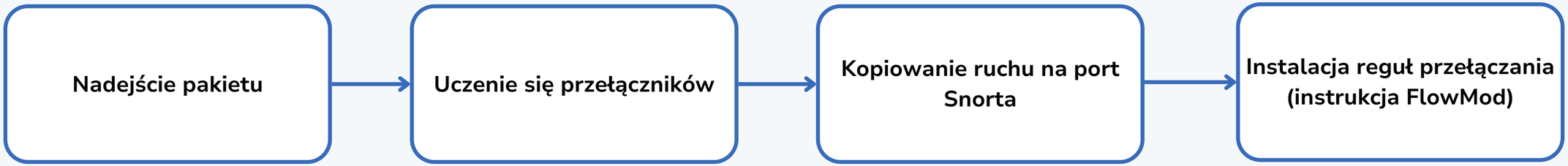
ALGORYTM DZIAŁANIA

FAZA I - INICJALIZACJA SIECI I KONTROLERA



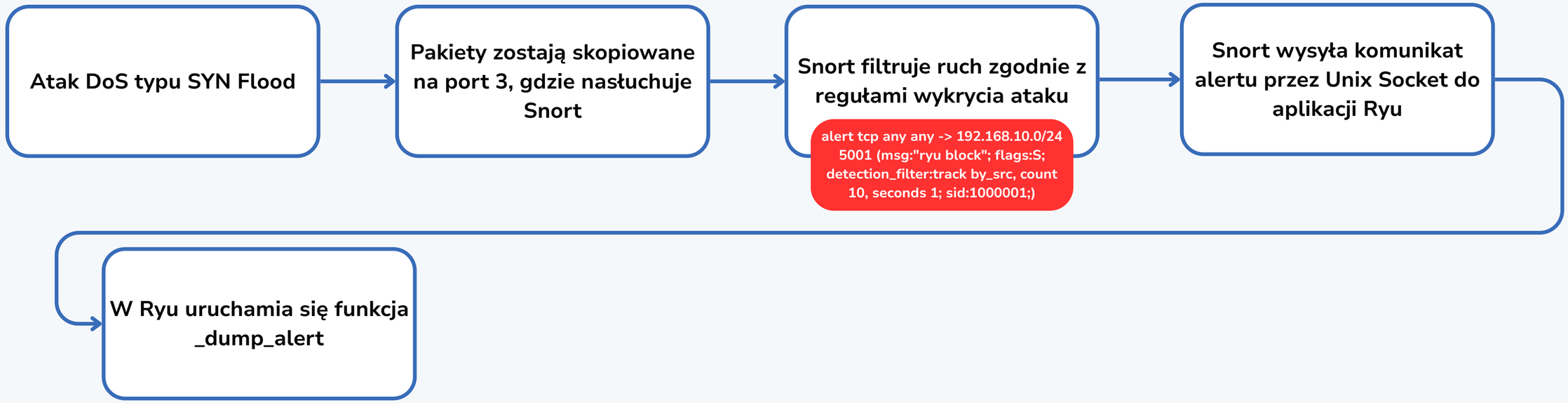
ALGORYTM DZIAŁANIA

FAZA II- NORMALNY RUCH I KOPIOWANIE DO SNORTA



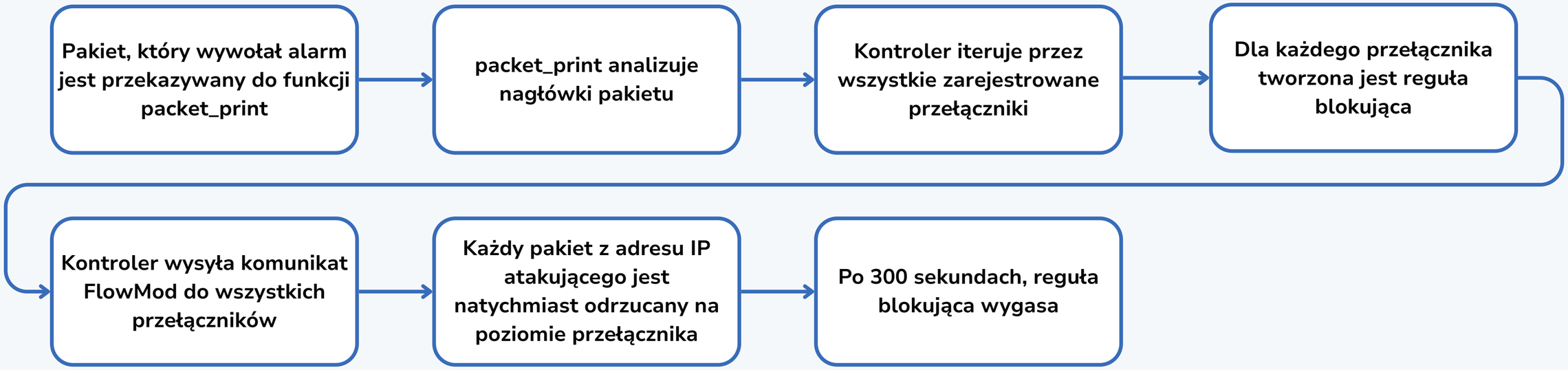
ALGORYTM DZIAŁANIA

FAZA III - WYKRYCIE ATAKU



ALGORYTM DZIAŁANIA

FAZA IV - REAKTYWNA BLOKADA



ŹRÓDŁA

1. Analysis and Review of TCP SYN Flood Attack on Network with Its Detection and Performance Metrics - Hrishikesh Shriram Salunkhe, Prof. Sanjay Jadhav, Prof. Vijay Bhosale. International Journal of Engineering Research & Technology (IJERT). 2017
2. SDN-Based Intrusion Detection System for Early Detection and Mitigation of DDoS Attacks - Pedro Manso, José Moura, Carlos Serrão. 2019
3. https://ianpeter.medium.com/denial-of-service-dos-attack-and-detection-using-snort-90ae68667822