Wykrywanie i blokowanie ataku DoS w sieci SDN z użyciem Snort i kontrolera Ryu

Przygotowanie sieci:

1. Uruchom kontroler ryu z simple_switch_stp_13
2. Uruchom Snort w trybie IDS (Intrusion Detection System)
3. Uruchom topologię mininet:
   -6 hostów
   -4 switche leaf
   -2 switche spine
4. Switche łączą się z kontrolerem Ryu

Działanie sieci:

1. Na każdym switchu leaf tworzymy port mirrorujący pakiety do SNORT
2. Pakiet trafia do adresu docelowego a jego kopia trafia równolegle do SNORT
3. Kontroler Ryu odbiera PacketIn i odczytuje MAC src, dst, in_port celem zapisania ich w tablicy

   mac_to_port[dpid][src] = in_port

4. SNORT analizuje nagłówki i zawartość pakietu i porównuje z regułami IDS
5. W przypadku wykrycia ataku SNORT generuje alert zawierający informacje o typie ataku i adresach IP/MAC źródłowym i docelowym
6. SNORT zapisuje alert do pliku zewnętrznego, okresowo monitorowanego przez kontroler Ryu skryptem
7. Kontroler Ryu odczytuje alert i informacje o IP/adresie MAC
8. Korzystając z tablicy mac_to_port Ryu identyfikuje przełącznik i port z którego pochodzi atak
9. Ryu tworzy regułę OpenFlow z wysokim priority celem dropowania ataku
10. Reguła jest wysyłana do najbliższego źródłu switcha
11. Pakiety ataku są dropowane na przełączniku
12. Sieć kontynuuje działanie pod monitoringiem SNORTa