S nástupem cloud computingu, kontejnerů a horizontálně škálovatelné infrastruktury, se nedílnou součástí datových center staly softwarově definované sítě (SDN). Jedním z běžně nasazovaných řešení je Kubernetes a Open vSwitch (OVS). V této diplomové práci hledáme možná výkonnostní omezení OVS při použití v rámci Kubernetes. Zaměřujeme se na problémy způsobené neobvyklým síťovým provozem. Výsledkem je objev několika typů paketů způsobujících nadměrné zatížení uzlů clusteru. Jako hlavní příčinu jsme identifikovali řadu filtračních pravidel v OpenFlow a chybu v návrhu OVS, která brání jejich efektivnímu vyhodnocování. Při specifické konfiguraci systému toto potenciálním útočníkům umožňuje využít objevenou neefektivitu k praktickému Denial-of-Service útoku na místní uzel clusteru, který způsobí kompletní síťový výpadek pro všechny kontejnery.