Implementácia firewallu založeného na Openflow protokole

Architektúra komunikačných systémov

Beňo Dávid

Harvan Šimon

2017/2018

FIIT-IT

# Obsah

[Obsah 2](#_Toc496685356)

[1. Úvod 3](#_Toc496685357)

[2. Analýza 3](#_Toc496685358)

[2.1 Analýza článku 3](#_Toc496685359)

[2.2 Technológie 3](#_Toc496685360)

[2.2.1 Mininet 3](#_Toc496685361)

[2.2.2 Firewall 4](#_Toc496685362)

[2.2.3 SDN 4](#_Toc496685363)

[2.2.4 Ryu 4](#_Toc496685364)

[2.2.5 OpenFlow protokol 4](#_Toc496685365)

[2.2.6 REST API 4](#_Toc496685366)

[3. Návrh riešenia 5](#_Toc496685367)

# 1. Úvod

Softvérovo definované siete (SDN) sú technológia, ktorá bude jadrom sietí ďalších generácií. Veľa spoločností a organizácií začalo používať SDN aplikácie. Toto dáva administrátorom flexibilitu pri implementovaní vlastných sieti. Ale zároveň vyvstávajú nové bezpečnostné problémy. Aby sme mohli zabezpečiť SDN siete potrebujeme silný firewall. Aktuálne už existujú firewally, ale majú určite nevýhody. Jeden z hlavných nedostatkov existujúcich riešení je, že sú umiestnené na jednom centrálnom zariadení a celý firewall zlyhá, ak zlyhá jedno zariadenie. Ďalší nedostatok existujúcich riešení je, že väčšina z nich sú firewall-y druhej vrstvy. V tomto článku implementuje distribuovaný firewall, kde sa každý OpenFlow prepínač v sieti môže správať ako firewall. Navyše bude tento firewall zvládnuť prevádzku protokolu TCP, UDP a ICMP. Testovali sme tento firewall pomocou emulátora Mininet, ktorý je nainštalovaný v Ubuntu 14.04 nainštalovaným pod VirtualBox. Používame POX riadič založený na Pythone. Táto práca je rozšírením našej predchádzajúcej práce na programovateľných firewall-och.

# 2. Analýza

## 2.1 Analýza článku

## 2.2 Technológie

V tejto kapitole sú popísané technológie, ktorými budeme v našom projekte pracovať.

### 2.2.1 Mininet

Mininet je emulátor siete, ktorý vytvára sieť virtuálnych hostov, prepínačov, ovládačov a odkazov. Mininet hostovia prevádzkujú štandardný sieťový softvér Linux a jeho prepínače podporujú OpenFlow pre vysoko flexibilné vlastné smerovanie a softvérové siete. Spoločnosť Mininet podporuje výskum, vývoj, učenie, prototypovanie, testovanie, ladenie a všetky ostatné úlohy, ktoré by mohli mať prospech z úplnej experimentálnej siete na prenosnom alebo inom počítači.

Mininet poskytuje jednoduchý spôsob, ako dosiahnuť správne správanie systému (a v rozsahu podporovanom vaším hardvérom, výkonom) a experimentovať s topológiami. Mininetové siete pracujú so skutočným kódom vrátane štandardných sieťových aplikácií Unix / Linux, ako aj skutočného jadra Linuxu a sieťového zásobníka.

Z tohto dôvodu sa kód, ktorý vyvíjame a otestujeme v službe Mininet, pre radič OpenFlow, zmenený prepínač alebo host, môže prejsť na skutočný systém s minimálnymi zmenami, pre testovanie v reálnom svete, hodnotenie výkonnosti a nasadenie. Dôležité je to, že návrh, ktorý pracuje v službe Mininet, sa zvyčajne môže presunúť priamo na hardvérové prepínače pre presmerovanie paketov line-rate.

### 2.2.2 Firewall

Brána firewall je sieťový bezpečnostný systém založený na hardvéri alebo softvéri, ktorý používa pravidlá na kontrolu prichádzajúcej a odchádzajúcej sieťovej prevádzky.

Brána firewall funguje ako bariéra medzi dôveryhodnou sieťou a nedôveryhodnou sieťou. Firewall kontroluje prístup k zdrojom siete prostredníctvom pozitívneho modelu kontroly. To znamená, že jediná prevádzka povolená na sieť je definovaná v pravidlách brány firewall - všetka ďalšia prevádzka bola zamietnutá.

### 2.2.3 SDN

Softvérovo definovaná sieť (SDN) je zastrešujúcim výrazom, ktorý zahŕňa niekoľko druhov sieťových technológií zameraných na to, aby bola sieť agilná a flexibilná ako virtualizovaná serverová a ukladacia infraštruktúra moderného dátového centra. Cieľom SDN je umožniť sieťovým inžinierom a administrátorom rýchlo reagovať na meniace sa požiadavky.

V sieťach definovaných softvérom môže správca siete tvarovať prevádzku z centralizovanej ovládacej konzoly bez toho, aby sa musel dotýkať jednotlivých prepínačov a môže poskytovať služby všade tam, kde sú potrebné v sieti, bez ohľadu na to, aké konkrétne zariadenia server alebo iné hardvérové súčasti sú pripojené k sieti. Kľúčovými technológiami implementácie SDN sú funkčné oddelenie, sieťová virtualizácia a automatizácia prostredníctvom programovateľnosti.

### 2.2.4 Ryu

Ryu kontrolór je otvorený kontrolór pre SDN siete, ktorý je navrhnutý tak, aby zvyšoval agilitu siete tým, že umožňuje jednoduchú správu a spôsob kontrolovania prevádzky. Vo všeobecnosti je kontrolór „mozog“ prostredia SDN, oznamuje informácie smerom k prepínačom a smerovačom ale aj aplikáciám a API na severi.

Ryu poskytuje softvérové komponenty s dobre definovanými aplikačnými programovými rozhraniami (API), ktoré uľahčujú vývojárom vytváranie nových aplikácií pre správu a riadenie siete. Tento prístup komponentov pomáha organizáciám prispôsobiť nasadenia tak, aby vyhovovali ich špecifickým potrebám prevádzky. Vývojári môžu rýchlo a ľahko upraviť existujúce komponenty alebo implementovať svoje vlastné, aby zabezpečili, že základná sieť môže spĺňať meniace sa požiadavky svojich aplikácií.

Zdrojové kódy ryu sú dostupné na serveri github a sú spravované Ryu komunitou.

### 2.2.5 OpenFlow protokol

### 2.2.6 REST API

# 3. Návrh riešenia