УДК 004.7, 004.732 **Г.О. Гринкевич**

АСПЕКТИ БЕЗПЕКИ ТА КОНФІГУРАЦІЯ НЕСПРАВНОСТЕЙ ПРИ РОЗГОРТАННІ SDN МЕРЕЖ

У даній статті наведено проблеми та дано короткий огляд рішень, запропонованих для вирішення питань управління мережею, які необхідні для оперативного використання в SDN. Проведені дослідження, що дають повне уявлення про потенційні і відкриті питання, що стосуються OpenFlow на основі архітектури SDN. Проаналізовано ряд проблем, які необхідно вирішити, коли оператори розгортають SDN в своїх мережах.

Ключові слова: програмно-конфігуровані мережі, управління, мережа, безпека даних, OpenFlow, SDN

Вступ

Поява програмованості в комп'ютерних мережах долає існуючі обмеження, що випливають з апаратних обмежень і патентованого програмного забезпечення. У порівнянні з традиційними мережами, програмованість збільшує гнучкість, що раніше не могло використовуватися через обмеження, що накладаються продавцями. У той час як мережеві оператори отримують вигоду від цієї нової свободи, виникають нові проблеми, пов'язані з управлінням мережі.

Сучасні рішення в області мережевого управління були розроблені для моделі мережі, в якій програмне забезпечення використовується в основному в формі для вбудованих систем. Це особливо відноситься до комутаторів і маршрутизаторів, які традиційно є непрограмованими мережевими пристроями, що містять дані управління, у площині управління. З останніми концепціями програмного забезпечення, де визначені Networking і OpenFlow, функціональність таких пристроїв тепер може бути заснована на програмному забезпеченні, що знаходиться на централізованій мережі контролеру [1]. Це збільшує гнучкість, оскільки нова функціональність залежить від вибору користувача мережевих додатків замість пристрою, що визначається постачальниками.

У той час як мережева програмованість дозволяє впровадження нових методів, що не були можливі за старої конструкції схеми, програмно не визначені мережеві архітектури вимагають нових рішень для управління мережею. Далі будуть розглянуті аспекти управління мережею, які необхідні для оперативного використання в SDN.

Основна частина

Конфігурація мережі. Комп'ютерні мережі складаються з ряду мережевих пристроїв, де кожен пристрій вимагає конфігурації специфічної до мережі та сценаріїв додатків. Типові дані конфігурації включають в себе загальні настройки, такі як IP-адреса і маску підмережі, а також дані протокольних параметрів. Вони можуть бути або відредаговані вручну за допомогою інтерфейсу командного рядка (англ. Command Line Interface, CLI) сценаріїв, або шляхом використання протоколів управління. Підстава для такого протоколу забезпечується тим, що він швидко стає неможливим оператору для читання або редагування параметрів вручну на всіх мережевих пристроях.

Протокол OpenFlow зосереджується на потоці на основі механізму переадресації і не забезпечує вирішення питання налаштування конфігурації мережевих пристроїв від пункту (s), як показано на рис. 1. Протокол OF-Config дозволяє зробити наступні настройки, щоб бути налаштованим на OpenFlow з підтримкою перемикачів:

- призначення одного або декількох контролерів до комутатора;
- видозміна властивостей інтерфейсу;
- конфігурація з сертифікованих для безпечного обміну даними з контролером;
- визначення можливостей комутатора;
- конфігурація протоколів тунелювання.

Протокол OF-Config заснований на NETCONF (RFC 6241), опублікований в 2006 році в якості транспортного протоколу. Він використовує універсальну мову моделювання даних під назвою YANG (RFC 6020 [2]), яка являє собою структури даних в розширювані мови розмітки

(XML)-на основі кодування даних. YANG можуть бути використані для моделювання конфігурації і даних про стан мережеви з елементів.

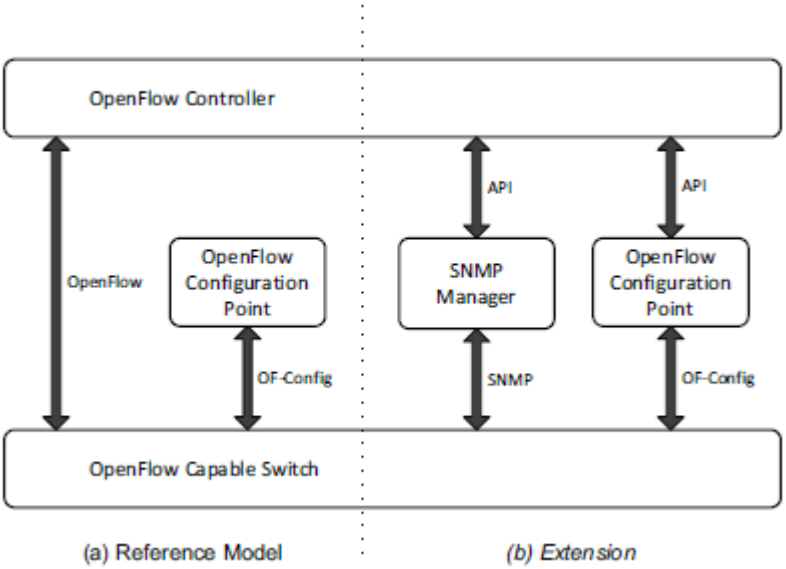

Рис.1. Пропоноване розширення еталонного режиму OpenFlow. Включає в себе API-інтерфейси для мережевого контролера для того, щоб отримати доступ до MIBs через SNMP і конфігурацію перемикача через OF-Config

SNMP є визначеним в RFC 1157 [3] і є найбільш поширеним протоколом для мережевого моніторингу та обробки помилок. Беруть участь всі мережеві пристрої, які визначені як мережеві елементи, можуть бути опитані від станції управління мережею адміністратора (NMS) для читання або зміни параметрів при наявності дозволу. Для структурування і зберігання даних в мережевих елементах, SNMP використовує структуру дерева, яке визначено в якості інформаційної бази управління (англ. Management Information Base, MIB) [4]. Таке дерево можна розглядати як віртуальну базу даних, що містить об'єкти, які доступні через унікальний об'єкт ідентифікаторів (Object Identifier, OID), який ідентичний на всіх мережевих пристроях.

Перевагою OID є те, що один запит був оброблений всіма мережевими пристроями, які підтримують такий об'єкт. У разі величезної мережі, опитування через SNMP створює додаткове навантаження на мережу. В свою чергу MIBs надсилає повідомлення про стан тільки в разі несправності.

Незважаючи на те, що SNMP дозволяє використовувати нові значення, які будуть встановлені в MIB, він рідко використовується для конфігурації через незручні процедури, що необхідні для досягнення цієї мети. Специфічні MIB для мереж на базі OpenFlow ще належить розробити, але вони необхідні, щоб дозволити операторам керувати такими мережами за допомогою протоколу SNMP. Функції, які повинні підтримувати такий MIB, аналогічні тим, які є в Specі для OF-Config

Як вже говорилося вище, SNMP протоколи OF-Config можуть використовуватись для доступу до конфігурацій даних на комутаторі. Сам мережевий контролер також може запросити мережеві параметри, які доступні тільки через SNMP або OF-Config. Наприклад, завантаження процесора і дані про споживання пам'яті можуть бути необхідні для балансування навантаження додатків. Тому необхідно визначати API-інтерфейси, які дозволяють проводити обмін даними налаштуванням між мережним контролером до точок конфигурацій (OF-Config) або станції управління мережею (SNMP), як показано на рис.1 . Наприклад, контролер може послати запит, що містить відповідний ідентифікатор об'єкта (наприклад, навантаження на центральний процесор) на станцію управління мережею, яка ініціює запит через SNMP до комутатора, для того, щоб зробити запит з MIB. Така концепція

вимагає, щоб контролер і задіяні пристрої модифікувалися для підтримки API. Це може бути забезпечено шляхом стандартизації таких інтерфейсів API, щоб підвищити визнання розробниками і постачальниками.

Є і свої недоліки. Управління включає в себе всі методи, які використовуються для виявлення, виділення і виправлення помилок в комп'ютерних мережах. Зведення на мінімум часу виявлення несправності є обов'язковим для мережевих операторів, з тим щоб зменшити вартість збою в мережі. У якості єдиної точки відмови мережевий контролер є ризиком, так як відмовляють всі мережеві пристрої. Для підвищення надійності мережі резервний контролер повинен бути забезпечений, щоб взяти на себе відповідальність управління в разі інциденту. Таке рішення вимагає синхронізації в режимі реального часу між двома мережевими контролерами з тим, щоб відобразити поточний стан мережі і скоротити час простою після збою до мінімуму. Інформація синхронізації стосується контролера і мережевих послуг мережі.

На додаток до розгортання одного або декількох контролерів резервного копіювання для підвищення надійності, виділені контролери можуть бути розгорнуті в мережі. Такий поділ мінімізує ризик того, що несправність в одному мережевому додатку буде вражати мережі вцілому. Проте, такий поділ створює додаткову складність, якщо застосуваня потрібно, щоб спілкуватися один з одним.

Крім самого контролера мережі, збої на мережевих пристроях повинні бути виявлені в цілях пом'якшення їх наслідків. Це може бути досягнуто за допомогою системи прогнозування, заснованої на аналізі системних повідомлень, щоб передбачити певні системні події [5]. Контролер мережі через свою централізовану позицію дозволяє збирати системні події для моніторингу мережі. Широкий діапазон подій може бути проаналізованим кореляцією двигуна несправностей для виявлення помилок, які характеризуються кількома низькорівневими подіями [6].

Перший підхід полягає в розгляді комутаторів і маршрутизаторів як зондів, що поширюють повідомлення про помилки мережевого контролера. Такий пасивний режим вимагає, щоб комутатор був здатен посилати таку подію. Наприклад, мережевий пристрій може відправити меседж про помилку з використанням протоколу OpenFlow в разі несправності. У разі виходу з ладу пристрою або каналу управління, мережевий контролер не може отримати інформацію про подію. Активний режим дозволяє уникнути цього опитування мережевих пристроїв. Це реалізується в OpenFlow шляхом відправки запитів між комутаторами мережевих пристроїв або каналу управління, або мережевого пристрою.

Оскільки мережеві пристрої в SDN не мають площини управління, помилки обмежені площиною даних, зменшуючи кількість можливих несправностей в порівнянні з не-SDN. Типова помилка на площині даних пов'язана з потоком таблиці перемикача. В не-SDN адресна пам'ять комутатора (англ. Computer-aided manufacturing, CAM) зберігає для кожного джерела MAC-адресу фізичного порту, через який пристрій може бути досягнутий. Зловмисник може використовувати цю ситуацію шляхом відправки пакетів з випадково підробленого джерела MAC-адрес, щоб вразити таблиці записів (MAC flooding attack). Повна таблиця змушує переключитися в режим безпеки, який передає всі пакети з усіх інтерфейсів. Це дозволяє зловмисникові зчитувати трафік з усіх хостів, підключених до цього комутатора. У SDN подібна атака можливива також. Споживаючи всю виділену пам'ять, зарезервовану для потоку таблиці, зловмисник може запобігти новим записам, що можуть бути встановлені на перемикачі.

Інша мета управління несправностями, зробити мережі більш автономними, наприклад, що робить їх здатними автоматично реагувати на невдачі техніки безпеки (наприклад, Брандмауер). У непрограмованих мережах це вимагає ручного втручання адміністратором для того, щоб розгорнути резервну систему, як показано на рис.2 У SDN це може бути автоматизованим шляхом поновлення потоку записів на відповідних перемикачів для того, щоб змінити маршрут трафіку до пристрою захисту. Це зводить до мінімуму перерви для

користувачів або мережевих сервісів. Перед тим як це може бути зроблено, відмова має бути виявленою. Це може бути досягнуто або шляхом опитування, або IDS, отримавши відповідне повідомлення про помилку. Крім того, контролер мережі може аналізувати статистику потоку записів, які використовуються для пересилання трафіку над пристроєм захисту. Незмінна кількість прийнятих пакетів / байтів або потоку, який досягає час простою можна вважати показником того, що зв'язок порушено.

Мережева безпека є обов'язковою для будь-якого оператора мережі для того, щоб зірвати атаки, які надходять від зловмисників, розташованих в Інтернеті або в мережі оператора (тобто інсайдерських атак). Таким загрозам, як правило, протистоять розгорнуті в мережі різні види технічної безпеки, як показано на рис. 2. Механізми таких систем мають загальну структуру. Після прийому пакетів на мережевому інтерфейсі, дозволяючи нерозбірливий режим, заголовок і корисне навантаження аналізуються і порівнюються з відомими підписами, які визначаються як правило, в конфігурації файлів. У разі збігу, дія яка застосовується до пакету, залежить від типу пристрою захисту. Для датчиків, таких як система виявлення вторгнень (IDS), які працюють в пасивному режимі, синхронізовані результати, в повідомленні, яке записується в журнал файлів, що описують дію разом зі своїм потоком інформації для подальшої перевірки. Системи запобігання вторгнень (International Prostate Symptom Score, IPSS) або файли rewalls працюють в активному режимі, що дозволяє пакетам бути заблокованими, щоб запобігти досягнення цільового хоста. Через апаратні обмеження один пристрій може обробляти тільки обмежену кількість пакетів в секунду. Це призводить до надлишковості трафіку в мережі, або збільшення вартості в міру розгортання додаткових пристроїв.

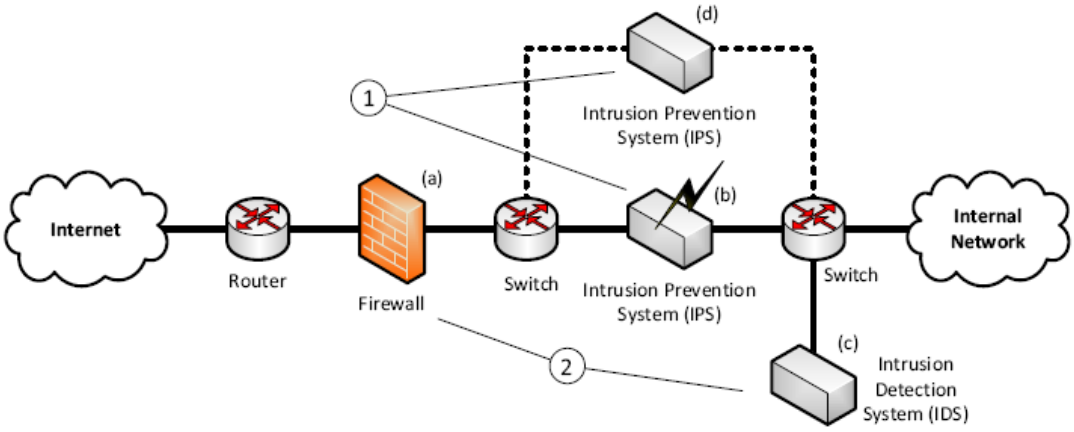

Рис. 2 Приклад мережевої безпеки в не-SDN. (1) техніка безпеки (a, b, c, d) не може адаптуватися до збоїв автоматично шляхом активації альтернативного пристрою. (2) Ні синхронізація між брандмауером, ні IDS набори правил не збільшують шанс мікро-конфігурації. Крім того, атаки не можуть активувати контрзаходи в сусідніх системах, наприклад, шляхом Брандмауер Recon конфігурацією.

Хоча IDS може ідентифікувати атаки, він не може блокувати їх. Оскільки оновлення правил набору в Брандмауер або IPS займає багато часу і може виявитися неможливим при коли відбувається напад, мережа не може бути захищена належним чином в такій ситуації. Змінюючи експедиторську дію потоку від входу, перемикачі на основі OpenFlow можуть бути використані, щоб блокувати трафіки, отже, можуть розглядатися як розподілений Брандмауер. Це дозволяє контролеру мережі реагувати на атаки в реальному масштабі часу, зупинивши трафік від противника або по периметру мережі, або на найближчому комутаторі, щоб ізолювати атакуючого.

Крім аналізу трафіку на виділених пристроях безпеки сам мережевий контролер може перевіряти пакети до певної міри. Це може бути досягнуто, оскільки перша пачка будь-якого

потоку, який не може бути узгоджений з існуючим потоком записів, надсилається в мережі контролером, інкапсульованого в повідомленні з комутацією пакетів. Інформація заголовка пакета витягується для того, щоб визначити відповідні параметри, які використовуються для установки нового потоку запису для цього типу пакета. Та інформація про пакет може отримати більш повної обробки мережевих сервісів і бізнес-додатків. Наприклад, аномалії виявлення алгоритмів або білі списки можуть бути використані для визначення того, чи містить пакет щось шкідливе або походить від злочинного джерела. Якщо результат позитивний, комутатор може блокувати трафік і заблокувати вхід таких пакетів в мережу. Другий варіант –це реалізація концепції багатошарової безпеки, наприклад для пересилання пакетів від невідомих джерел за альтернативним маршрутом через мережу, відокремлену від даних зв'язку. Розробка таких додатків знову залежить від API, що несе відповідальність за забезпечення того, що інформація заголовка пакета доступна з бізнес-додатків.

Виявлення несправностей в мережах на базі OpenFlow вимагає адекватного рішення моніторингу. На додаток до подій, які специфікуються протоколом OpenFlow, мережеві потоки є важливим джерелом інформації, яка може бути оброблена на централізованій площині управління. Ми зацікавлені у визначенні пов'язаних параметрів потоку, які можна розглядати в залежності від обставин сприятливих для виявлення аномалій або класифікацій трафіку. Мережеві потоки також можуть бути використані для визначення логічної топології мережі. Це вимагає визначення метрики, що можуть бути використані для аналізу розподілу трафіку всієї мережі. Ця інформація в подальшому може використовуватися мережевими службами, наприклад, щоб реалізувати балансування навантаження або для виявлення відмов мережі.

Критичні помилки можуть також виникати на комутаторі і бути наслідками для пересилання пакетів. Відповідний механізм в цьому випадку це потік-таблиця, яка визначає відношення між заголовком пакетів полів і фізичнм портом. Оскільки число записів на потік таблиці обмежений, зловмисники можуть спробувати видалити таблиці з непотрібних записів (MAC flooding attack), щоб включити відмовостійкий режим. Незважаючи на те, існують методи ослаблення впливу в не-SDN, наслідки такої атаки в мережах на базі OpenFlow ще належить досліджувати. Проаналізуємо, наскільки повний потік-таблиця може впливати на мережевий пристрій і мережний контролер.

Контролер на основі виявлення вторгнень. З точки зору безпеки, SDN відкриває нові способи перемоги атаки шляхом надання можливості моніторингу. Один аспект стосується огляду пакету, який може бути реалізований на самому мережному контролері. Це розумно, тому що повідомлення управління інкапсолюється. Перший пакет нового потоку посилається в контролер. Аналізуючи такі пакети, ніяких додаткових накладних витрат зв'язку не понесено, а діапазон такої інспекції має охопити всі рівні протоколу для того, щоб визначити відповідні функції трафіку.

Мета даної роботи полягає у визначенні потенціалу для такого контролера на основі перевірки пакетів шляхом подання типових сценаріїв додатків. Механізм інспекції може бути реалізований в якості мережевих послуг, наприклад, додаток безпеки, що забезпечує оперативний захист від певного типу атаки. Інформація, витягнута з конкретного потоку також може бути використовуватися для того, щоб забезпечити різні рівні безпеки. Наприклад, трафік з специфічного хоста може бути прокладений через різні дороги.

Налагодження мережі. Концепція SDN вимагає нових інструментів для налагодження мережі і аналізу першопричин. Це відбувається тому, що всі мережеві події обробляються в централізованій площині управління, яка додатково поділяється на різні мережеві послуги. Однією з головних завдань керуючої мережі це притоки, що реалізуються конфігурацією мережевих пристроїв і установкою потоку записів. Для того, щоб забезпечити повне стеження за потоком входу відповідальних мережевих послуг,пропонується інструмент, який може забезпечити таку функціональність. Він забезпечує автоматизований підхід для того, щоб гарантувати надійність, ремонтопридатність і масштабованість мережі.

Висновки

Концепція SDN нова для контролю і управління комп'ютерними мережами. Навіть незважаючи на те, гнучкість такої інфраструктури значно більша, ніж з непостійним SDN, категорії управління мережею, підсумовані по FCAPS [7] як і раніше існують і вимагають відповідних рішень для сценарія SDN. В даній статті проаналізовано ряд проблем, які необхідно вирішити, коли оператори розгортають SDN в своїх мережах. Наприклад, самонастроювання таких мереж є більш важким, ніж для не-SDN, оскільки кожен мережевий пристрій повністю залежить від мережевого контролера. Те ж саме відноситься до каналу управління, який може бути або реалізований в смузі, або поза смугою режиму. Завдяки централізованій площині управління, управління відмовами спрощена, тому що всі мережеві події можуть бути оброблені в центральному місці на мережевому контролері. Налагодження таких мереж до цих пір немає відповідних інструментів. Будь-яке рішення повинно враховувати функціональні можливості мережевих послуг, а також події, які запускаються з мережевих пристроїв. З точки зору безпеки, мережевий контролер може відігравати різну роль для того, щоб відрізнити поведінку пересилання пакетів в мережі. Ця інформація може також привести до концепцій, які динамічно включають різні IDSS шляху потоку, для того, щоб проаналізувати конкретні зв'язки і адаптувати рівень безпеки для мережевого навантаження.

Література

1. Thomas A. Limoncelli OpenFlow: A Radical New Idea in Networking [Електронний ресурс] / Thomas A. Limoncelli // Communications of the ACM. — N. Y., 2012. — Т. 55, № 8. — С. 42-47 – Режим доступу : // http://queue.acm.org/detail.cfm?id=2305856 (02.06.2016 р.)

2. M. Bjorklund, YANG - A Data Modeling Language for the Network Configuration Protocol (NETCONF) (IETF RFC 6020) [Електронний ресурс] / M. Bjorklund // The Internet Society, Oct. 2010. – Режим доступу : // https://tools.ietf.org/html/rfc6020 (01.06.2016 р.)

3. J. Case, M. Fedor, M. Schoffstall, and J. Davin, A Simple Network Management Protocol (SNMP) (IETF RFC 1157). [Електронний ресурс] / J. Case, M. Fedor, M. Schoffstall, and J. Davin // The Internet Society, May 1990. – Режим доступу : https://tools.ietf.org/html/rfc1157 (15.07.2016 р.)

4. K. McCloghrie, D. Perkins, and J. Schoenwaelder, Structure of Management Information Version 2 (SMIv2) (IETF RFC 2578). [Електронний ресурс] / K. McCloghrie, D. Perkins, and J. Schoenwaelder // The Internet Society, April 1999. – Режим доступу : https://tools.ietf.org/html/rfc2578 (15.07.2016 р.)

5. A. Clemm and M. Hartwig. NETradamus: A forecasting system for system event messages. [Електронний ресурс] / Clemm and M. Hartwig // Network Operations and Management Symposium (NOMS'10), April 2010, pp. 623–630. – Режим доступу : http://www.bibsonomy.org/bibtex/228038810dfa0d28783bc7811694ba576/dblp (15.07.2016 р.)

6. A. Makanju, A. N. Zincir-Heywood, and E. E. Milios. Interactive learning of alert signatures in high performance cluster system logs. [Електронний ресурс] / A. Makanju, A. N. Zincir-Heywood, and E. E. Milios // Network Operations and Management Symposium (NOMS'12), 2012, pp. 52–60. – Режим доступу : http://ieeexplore.ieee.org/document/6211882/ (15.07.2016 р.)

7. FCAPS [Електронний ресурс] / Без автора // – Режим доступу : https://ru.wikipedia.org/wiki/FCAPS

Надійшла 25.07.2016 р. Рецензент: д.т.н., проф. Шевченко В. Л.