БЕЗПЕКА В ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖАХ (SDN)

Гришин С. О., ст. (гр. КВ-81мп, ФПМ КПІ ім. Ігоря Сікорського)

Анотація: Дана робота – це огляд технології SDN (програмно-конфігуровані мережі), її архітектури, функціонування та проблем безпеки, пов'язаних з архітектурою цього типу мереж.

Ключові слова: захист інформації, SDN, програмно-конфігуровані мережі, безпека SDN мереж, DoS-атаки.

Abstract: This work is an overview of the technology of SDN (software-configurable network), its architecture, operation and security issues related to the architecture of this type of network.

Keywords: information protection, SDN, software-configurable networks, SDN network security, DoS attacks.

Сучасні мережеві технології з кожним роком набирають все більших обертів у розвитку. Основними причинами, які сприяють такому прискоренню є підвищення вимог до швидкості передачі трафіку, власне збільшення цього трафіку, а також підвищення вимог до безпеки переданих даних.

Традиційні мережі мають складну структуру, що робить їх складними в адмініструванні. Для того, щоб додати та налаштувати новий пристрій в мережі, необхідно налаштувати кожен пристрій в цій мережі. Це реалізується за рахунок спеціальних протоколів, що ускладнює роботу всього стеку протоколів мережі [1].

Одним з витків розвитку сучасних мереж є SDN (Software-defined Networks – з англійської програмно-конфігуровані мережі). Дана технологія, в першу чергу, цікава для розподілених обчислень, так як дозволяє перенести всі управління мережею в єдиний модуль (контролер) управління і таким чином відокремити управління мережею від управління передачею даних в цій мережі. Також, це дозволить розділити два аспекти безпеки в цих мережах.

Взагалі безпека – це дуже широке поняття. Необхідно чітко визначити джерела небезпек в мережах:

– небезпечний контент;

– небезпечне з'єднання (тут варто зазначити, що з'єднання є небезпечним в разі, коли в нього вже втрутився зловмисник. До тих пір, з'єднання варто вважати вразливим, тобто таким, яке потенційно не має захисту від зловмисника).

Архітектура SDN-мереж передбачає відокремлення контролю передачі даних і контролю з'єднання. Таким чином, мережі SDN мають три рівні:

– рівень передачі даних – передавачі, комутатори, тобто пристрої, задача яких передавати трафік в мережі та надавати простий інтерфейс для взаємодії з ними верхнім рівням;

– рівень управління мережею – контролер або декілька контролерів, які управляють мережею, забезпечують з'єднання та передачу в мережі;

– рівень прикладних додатків – рівень, на якому функціонують прикладні програми, які використовують отримані дані, та/або передають дані через мережу [2].

Для забезпечення роботи такої архітектури, необхідний відповідний протокол, який буде комутувати рівні мережі. Одним із таких протоколів є Open Flow [3]. Він працює на наборі правил, які записані в його таблиці комутації.

Таким чином, контролер з'єднання виділений окремо від усіх елементів в мережі і є її самостійною частиною. Ще однією особливістю SDN є те, що контролери з'єднання є програмами на серверах, що значно спрощує додавання нових пристроїв до мережі та адміністрування існуючих. Але це також збільшує вразливість мережі, оскільки отримавши доступ до контролера, зловмисник отримує доступ до всієї мережі.

Насьогодні всі відомі атаки на мережі типу SDN тією чи іншою мірою базуються на тому, що в таких мережах єдиний відокремлений від всіх контролер. Атаки в мережах SDN можна поділити на такі види:

– атаки на топологію – підміна ARP-пакетів мережі, Faketopology, або перебудова топології мережі (або її частини). Під час атаки з підміною ARP-пакетів, контролер встановлює додаткові правила для потоків в мережі для перехоплення та обробки шкідливих даних.

–маніпулювання додатком: ця атака відбувається в площині прикладних програм. Використання вразливості додатків може спричинити несправність, зрив служби або «підслуховування» даних. Зловмисник може отримати доступ до контролера із високим привілеєм та виконувати незаконні операції.

– експлуатація API контролера: API програмного компонента може містити вразливі місця, які можуть дозволити хакерам отримувати несанкціоновану інформацію.

– сніферінг-трафіку – популярний метод для захоплення та аналізу мережевого трафіку. За допомогою сніферінгу, зловмисник може отримати інформацію про топологію мережі, адреси в ній, потоки тощо.

– підбір паролю за принципом «грубої сили». Цей метод вже застарілий, але інколи він може дати позитивний результат, якщо користувач мережі залишив стандартний пароль, наприклад, від своєї робочої станції. Зловмисник може перебором підібрати пароль до одного з компонентів мережі, а потім отримати контроль над усією мережею, через отриманий доступ до одного.

– атаки на контролер передачі даних – DoS-атака (Denial-of-Service – з англійської атака на відмову) контролера, переповнення пам'яті комутатора (TCAM exhaustion). Тут можливі два варіанти:

– комутатор отримує пакет та пересилає його повністю контролеру для аналізу;

– комутатор отримує пакет, буферизує його та пересилає контролеру тільки частину пакету із заголовками [4].

В обох випадках контролер змушений обробляти велику кількість даних, і не встигатиме обробляти інші запити від комутаторів, що може привести до великих затримок при передачі даних або навіть зупинити роботу контролера.

Проте, контролер в мережах SDN, за рахунок того, що це програма на сервері, може бути розширеним додатковими модулями для забезпечення безпечного функціонування мережі. Існують готові програмні засоби, наприклад, програма «AVANT-GUARD» для виявлення (D)Dos-атак. Захист від такого типу атак реалізується шляхом обмеженням ресурсів для конкретного прикладного додатку. Також, Yu Huang C. Inc запропоновано варіант захисту від таких атак шляхом аналізу статистики мережевого трафіку.

Архітектура мереж SDN суттєво відрізняється від існуючих, «класичних» мереж, а, отже, відрізняються і методи забезпечення безпеки в таких мережах. Поєднання централізованого управління і програмування мережі дозволяє підвищити ефективність засобів забезпечення безпеки мережі [5]. Централізований мережний контролер, який є критичним для нормального функціонування мережі, є дуже вразливим до різного типу атак, зокрема, (D)DoS-атак, спрямованих на контролер, які можуть привести до відмови всієї мережевої інфраструктури.

Висновки. Одним з найбільш ефективних засобів протидії (D) DoS- і скан-атакам в традиційних мережах передачі даних є системи виявлення вторгнень. Для мереж типу SDN також запропоновані методи виявлення атак типу (D)DoS та серверні додатки для аналізу трафіку для попередження таких атак. Оскільки SDN – програмні мережі, то одним із важливих факторів, які впливають на рівень захищеності мережі, є своєчасне оновлення патчів з базами вірусів та механізмами аналізу загроз.

Науковий керівник: Землянська О. В., ст. викл. (каф. ОППЦБ КПІ ім. Ігоря Сікорського)

Література

1. Смелянский Р. Л. Программно-конфигурируемые сети – Новый подход к построению компьютерных сетей / Р. Л. Смелянский.
2. Ehab Al-ShaerOpenflow random host mutation: transparent moving target defence using software defined networking. In Proceedings of the first workshop on Hot topics in software defined networks / E. A. J. J. Haadi, D. Qi.
3. TheRealStoryonSDNandNFVSecurity [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://blog.cimicorp.com/?p=2561.
4. Эволюция сети к SDN&NFV [Електронний ресурс]. – 2016. – Режим доступу до ресурсу: https://habr.com/post/307356.
5. Сетевые технологии SDN – SoftwareDefinedNetworking [Електронний ресурс]. – 2015. – Режим доступу: https://habr.com/company/muk/blog/251959.