УДК 621.382

# СЛУЖБИ БЕЗПЕКИ SDN

**Сікач Т.О.**
*Інститут телекомунікаційних систем КПІ ім. Ігоря Сікорського, Україна*
*E-mail: Nainek95@gmail.com*

**Software-Defined Networking Security Services**

We will discuss the limitations of existing systems and presents a possible SDN-based system to assert network resources by controlling unsafe and doubtful network traffic. We consider the main vulnerabilities of Software Defined Networks such as limitation inheritance and do some research of ways of solution those problems.

Програмно-конфігурована мережа ( SDN ) – це набір методів, що дозволяє користувачам напряму програмувати, організовувати, контролювати та керувати мережевими ресурсами за допомогою програмного забезпечення ( SDN аплікації). Вона переводить управління мережевими ресурсами на окремий мережевий елемент, а саме SDN контролер.

Контролер SDN використовує інтерфейс і керує розподілом мережевих ресурсів логічно-цетралізованим чином. Він також керує і налаштовує розподіленими мережевими ресурсами і надає абстрактні представлення мережевих ресурсів для аплікацій SDN. Аплікація SDN може налаштувати і автоматизувати операції абстрактних мережевих ресурсів в програмному режимі через інтерфейс.

Перейдемо до загроз безпеки, через зростання складності мережевих атак, з наслідуванням служб безпеки стає складно справлятися в автономному режимі.

SDN був введений, щоб зробити мережі більш контрольованими. І ця технологія повинна автономно справлятися з такими мережевими атаками у вигляді підказок, або у режимі запит-відповідь. Цілі та вимоги для підтримки захисту мережевих ресурсів забезпечуються через SDN сервіси безпеки використовуючи загальний інтерфейс для функцій мережевої безпеки.

В якості вирішення цих проблем, пропонується два варіанти використання служб безпеки, таких як централізована брандмауер система і централізована система попередження та зменшення наслідків після атак на відмову (DDoS).

Для централізованої системи брандмауера виникають обмеження з наслідуванням в брандмауерах з точки зору гнучкості та витрат на адміністрування. Оскільки в більшості випадків керування доступом в

брандмауері виконується вручну, складно додати правила управління доступу, відповідно до нових мережевих атак швидко та автономно. Таким чином, ця ситуація вимагає великих витрати на адміністрування.

Для системи попередження та зменшення наслідків після атак на відмову, виникають такі ж самі обмеження щодо успадкування з точки зору гнучкості та витрат на адміністрування. Так як в багатьох випадках, конфігурація мережі для попередження і зменшення наслідків виконується вручну, виникає складність в динамічній конфігурації мережевих пристроїв для обмеження і контролю підозрілого мережевого трафіку для атак на відмову.

На рис.1 показана структура  для служб безпеки SDN. Як показано на рисунку, аплікації для служб безпеки ( брандмауер та система боротьби з атаками на відмову ) виконується поверх SDN контролеру. Коли адміністратор нав'язує політики безпеки для служб безпеки через інтерфейс аплікації, SDN контролер генерує відповідну політику доступу ( або конфігурацію мережі ) для задоволення політики безпеки в автономному режимі та режимі запит-відповідь. Згідно згенерованих правил політики контролю, мережеві ресурси, такі як комутатори, вживають заходи щодо пом'якшення мережевих атак, наприклад скидання пакетів з підозрілими шаблонами.

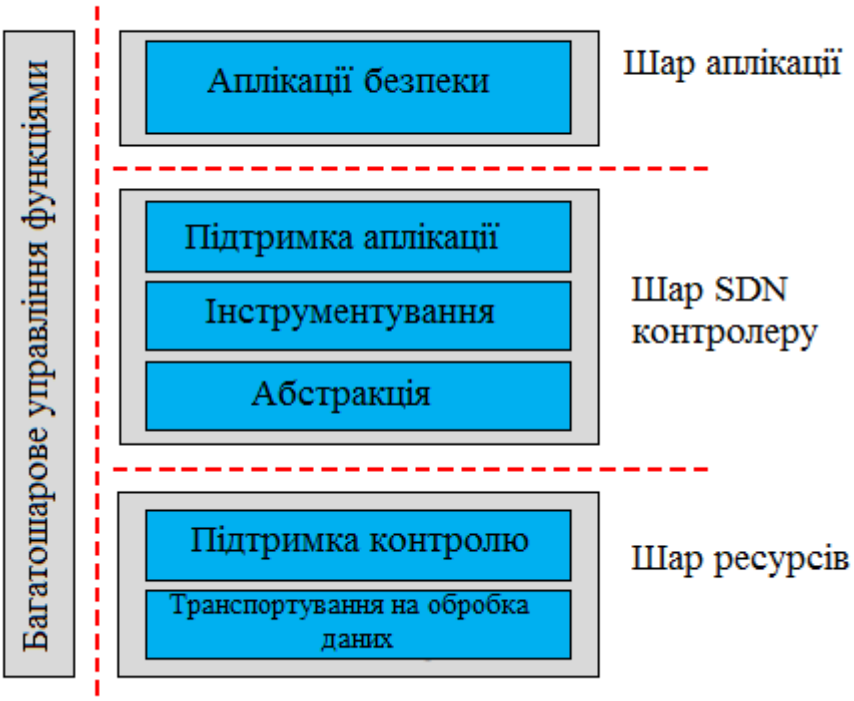


Рис. 1. Високорівнева архітектура для служб безпеки SDN.

Питання дослідження: Для запобігання несанкціонованого управління комутаторами, безпечний і справжній, автентичний канал між SDN контролером і комутаторами повинні бути встановлені перемикачі. Тобто нам потрібно розглянути управління ключами для забезпечення безпечного зв'язку між ними.

Централізований сервер ( SDN контролер ) буде страждати від єдиної точки відмови або компромісу. Без захисту контролеру SDN, неможливо розгорнути служби безпеки на основі SDN.

Для підтримки служб безпеки SDN, нам необхідно розглянути зміни в існуючих комутаторах і протоколах SDN.

Теоретично SDN здається розумною архітектурою для забезпечення централізованих служб безпеки. Однак, коли ми розглядаємо множину комутаторів і хостів, зв'язок між контролером SDN і комутаторами є потенційно слабкою ланкою, тому проблема маштабованості є актуальною.

Підтримка служби безпеки в тенденціях автономності та маштабованості, комутатори повинні інтелектуальними щоб здійснювати рішення відносно безпеки щодо атак. Отже це важливе питання на скільки інтелектуальними є комутатори з точки зору продуктивності та автономності.

Ефективні інтерфейси для функцій безпеки мережі, повинні бути реалізовані на базі NETCONF/YANG в середовищі віртуалізації мережі, таких як SDN комутатори можуть бути швидко зконфігурованими відповідно до вимог служб безпеки. Це можливо завдяки ефективній взаємодії між контролером безпеки і контролером SDN.

**Література**


1. Recommendation ITU-T Y.3300, “Framework of Software-Defined Networking,” ITU-T, Jun. 2014.
2. J. Jeong, H. Kim, and J. Park, “Requirements for Security Services based on Software-Defined Networking,” IETF draft-jeong-i2nsf-sdnsecurity-services-02, Jul. 2015.
3. R. Enns, M. Bjorklund, J. Schoenwaelder, and A. Bierman, “Network Configuration Protocol (NETCONF),” IETF RFC 6241, Jun. 2011.
4. Open Networking Foundation, “SDN Architecture,” ONF, Jun. 2014.
5. H. Kim and N. Feamster, “Improving Network Management with Software Defined Networking,” IEEE Communications Magazine, vol. 51, no. 2, pp. 114–119, Feb. 2013.