АНАЛІЗ ЗАСОБІВ МАРШРУТИЗАЦІЇ ЩОДО ПІДВИЩЕННЯ РІВНЯ МЕРЕЖНОЇ БЕЗПЕКИ У ПРОГРАМНО-КОНФІГУРОВАНИХ МЕРЕЖАХ

Плєхова Г.А.

Кафедра «Інфокомунікаційної інженерії ім. В.В. Поповського»,
Харківський національний університет радіоелектроніки, Україна

E-mail: hanna.pliekhova@nure.ua

Abstract

Currently, the deployment of such network architectures as Software-Defined Networks (SDN) is facing new cyber security threats that require developing and researching new specialized solutions to increase network security. An important place in the complex means of increasing network security, including SDN networks, is given to routing protocols. The conducted analysis of vulnerabilities of the SDN data plane and the functionality of routing means in terms of countering possible attacks showed the perspective of using secure routing under base scores of the vulnerabilities' criticality (CVSS) to increase the level of network security of the SDN data plane.

Наразі розгортання таких мережних архітектур, як програмно-конфігуровані мережі (Software-Defined Networking, SDN), стикається з новими загрозами кібербезпеці, які вимагають розробку та дослідження нових спеціалізованих рішень щодо підвищення рівня мережної безпеки [1]. Незважаючи на високу відкритість і можливості програмованості, архітектура SDN замінює традиційну мережу, проте збільшує кількість потенційних мережних атак, що призводить до нових проблем безпеки.

Завдяки зростаючому інтересу до SDN та широкому розгортанню програмно-конфігурованих мереж поступово виявляються їхні недоліки у боротьбі із загрозами кібербезпеці. Відповідно питання щодо безпеки тісно пов'язані з характеристиками SDN. Згідно з дослідженнями [2, 3], наступні аспекти роблять програмно-конфігуровані мережі вразливими до атак:

1. SDN контролер, що відповідає за централізований контроль мережею, має недостатні механізми захисту, через що стає ціллю зовнішніх зловмисних атак.
2. В процесі складної взаємодії пов'язаних між собою різноманітних прикладних програм і мережних застосунків між ними часто виникають конфлікти у правилах передавання потоків у межах площини даних.
3. Відсутність належних механізмів авторизації та автентифікації прикладних програм робить їх уразливими до атак з використанням зловмисного програмного забезпечення.
4. Існує певна недостатність засобів безпеки та шифрування в процесі комунікації між площиною управління та площиною даних. Отже, правила передавання потоків (flow rules) уразливі щодо зловмисного втручання під час їхньої публікації.

Очевидно, що об’єктами атак можуть бути пристрої різних рівнів мережі, і відповідно до чіткої багаторівневої архітектури SDN можна класифікувати загрози безпеці на різних рівнях [2, 3]. Дана робота присвячена аналізу загроз, об'єктів атак і потенційних рішень щодо підвищення рівня мережної безпеки на у площині даних SDN мереж засобами маршрутизації. Отже, площина даних складається з комутаторів та інших мережних пристроїв і головним чином відповідає за обробку даних, їх пересилання, відкидання, а також збір статистики. Функціонування площини даних відбувається на основі правил потоків, що надаються контролером мережі. Тоді як основними причинами проблем безпеки є власне архітектура SDN, зовнішні шкідливі атаки, недостатність контролю доступу та засобів шифрування.

На сьогоднішній день важливе місце у комплексі засобів підвищення мережної безпеки, у тому числі мереж SDN, відводиться протоколам маршрутизації, які потребують системної та

скоординованої взаємодії одночасно множини мережних елементів – SDN-комутаторів, і контролерів мережі під час формування (розрахунку) шляхів і правил потоків, вздовж яких має забезпечуватися необхідний рівень безпеки за обраними показниками або критеріями.

Отже, у напрямку безпечної маршрутизації проведено значну кількість теоретичних досліджень, починаючи від найпростіших емпіричних варіантів рішень до системних оптимізаційних підходів [4-7]. Так, у роботі [5] розроблено та досліджено модель безпечної маршрутизації з балансуванням навантаження в мережах на основі SD-WAN. Технологічне завдання безпечної маршрутизації з балансуванням навантаження було сформульовано у формі оптимізаційної задачі з квадратичним критерієм оптимальності. Така форма критерію дозволяє збалансувати частки потоків, що передаються в мережі. Тоді як у роботах [6, 7] пропонуються потокові моделі маршрутизації з урахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей. Основу моделі складають умови реалізації одно- та багатошляхової маршрутизації, збереження потоку та запобігання перевантаженню каналів зв'язку, а задача безпечної маршрутизації також сформульована як оптимізаційна. У моделі [6] для розрахунку маршрутних метрик використовуються вирази, які характеризують ризик інформаційної безпеки в каналах зв'язку мережі та відповідно до рекомендацій NIST враховують збитки від порушення конфіденційності та цілісності інформації, доступності мережного ресурсу у випадку використання наявних вразливостей; показники складності використання вразливостей на вузлах мережі та отримання доступу до мережних елементів та мережі загалом внаслідок використання зазначених уразливостей. Запропонований авторами підхід до формування маршрутних метрик може бути використаний під час комплексного врахування в процесі розв'язання задач маршрутизації як показників мережної безпеки, так і показників якості обслуговування.

Проведений аналіз вразливостей площини даних SDN і функціональних можливостей засобів маршрутизації щодо протидії можливим атакам показав перспективність використання засобів безпечної маршрутизації на основі базових метрик критичності вразливостей для підвищення рівня мережної безпеки площини даних SDN. Аналіз стандарту CVSS [8] щодо кількісного розрахунку рівня вразливості мережного обладнання довів доцільність його використання під час розробки та дослідження перспективних підходів до безпечної маршрутизації у площині даних програмно-конфігурованих мереж.

*Л*ітература:

1. *Sabella A., Irons-Mclean R., Yannuzzi M.* Orchestrating and automating security for the internet of things: Delivering advanced security capabilities from edge to cloud for IoT, Cisco Press, 2018. 1008 p.
2. *Liu Y., Zhao B., Zhao P., Fan P., Liu H.* A survey: Typical security issues of software-defined networking. China Communications. 2019. № 16(7). P. 13-31. DOI: https://doi.org/10.23919/JCC.2019.07.002
3. *Sagare A.A., Khondoker R.* Security Analysis of SDN Routing Applications. In: Khondoker, R. (eds) SDN and NFV Security. Lecture Notes in Networks and Systems, vol 30. Springer, Cham, 2018, P. 1-17. DOI: https://doi.org/10.1007/978-3-319-71761-6_1
4. *Лемешко О.В., Єременко О.С., Невзорова О.С.* Потокові моделі та методи маршрутизації в інфокомунікаційних мережах: відмовостійкість, безпека, масштабованість. Харків: ХНУРЕ. 2020. 308 с. DOI: https://doi.org/10.30837/978-966-659-282-1
5. *Yeremenko O., Persikov M., Lemeshko V., Altaki B.* Research and development of the secure routing flow-based model with load balancing. Проблеми телекомунікацій. 2021. № 2(29). С. 3-14. URL: https://pt.nure.ua/wp-content/uploads/2021/12/212_yeremenko_secure.pdf
6. *Євдокименко М.О., Шаповалова А.С., Шаповал М.М.* Потокова модель маршрутизації із врахуванням ризиків інформаційної безпеки за допомогою базових метрик критичності вразливостей. Проблеми телекомунікацій. 2020. № 1(26). С. 48–62. URL: http://pt.nure.ua/wp-content/uploads/2021/03/201_yevdokimenko_security.pdf
7. *Yevdokymenko M., Yeremenko O., Shapovalova A., Shapoval M., Porokhniak V., Rogovaya N.* Investigation of the Secure Paths Set Calculation Approach Based on Vulnerability Assessment. Workshop Proceedings of the MoMLeT+DS 2021: 3rd International Workshop on Modern Machine Learning Technologies and Data Science, June 5, 2021, Lviv-Shatsk, Ukraine. P. 207-217. URL: http://ceur-ws.org/Vol-2917/paper19.pdf
8. Common Vulnerability Scoring System v3.0: Examples, Forum of Incident Response and Security Teams, URL: https://www.first.org/cvss/examples