УДК 004.75:004.056.5
В. Стрихарський; О. Оробчук, доктор філософії
(Тернопільський національний технічний університет імені Івана Пулюя, Україна)

ЦЕНТРАЛІЗОВАНЕ УПРАВЛІННЯ ПОЛІТИКАМИ БЕЗПЕКИ У SDN ІЗ ВИКОРИСТАННЯМ МЕХАНІЗМІВ ФІЛЬТРАЦІЇ ДОСТУПУ

UDC 004.75:004.056.5
V. Strykharskyi; O. Orobchuk, PhD.

CENTRALIZED SECURITY POLICY MANAGEMENT IN SDN USING ACCESS FILTERING MECHANISMS

Програмно-визначені мережі (SDN) [1] є архітектурною основою сучасних хмарних платформ, віртуалізованих дата-центрів та 5G-інфраструктур, що робить їх привабливою ціллю для зловмисників. Централізоване керування трафіком, поділ на площини даних, керування та застосунків, а також активне використання API створюють розширену площину атак на контролер, канали взаємодії та мережеві функції. У таких умовах класичні фаєрволи зі статичними ACL та сигнатурні системи виявлення вторгнень виявляються недостатньо ефективними, погано масштабуються та не забезпечують потрібного рівня узгодженості політик безпеки.

У роботі запропоновано узагальнену модель активів SDN-інфраструктури, що охоплює площину даних, площину керування, площину застосунків, канали Southbound, Northbound і East–West, а також допоміжні сервіси. Для кожного класу активів систематизовано типові загрози. Запропоновано підхід до кількісної оцінки ризиків, що поєднує модифіковану метрику CVSS із методом аналізу ієрархій AHP. Такий підхід дозволив ранжувати сценарії атак і обґрунтовано визначати, які типи з'єднань мають контролюватися на рівні стану, а де достатньо статичних правил фільтрації. На основі отриманих результатів розроблено архітектуру SDN-фаєрвола із перевіркою стану з'єднання, орієнтованого на централізоване керування політиками. Фаєрвол реалізовано як набір додатків до контролера RYU [2] із зовнішнім оркестратором політик, що динамічно генерує правила OpenFlow для комутаторів Open vSwitch [3] з урахуванням поточного стану окремих сеансів. Логіку роботи фаєрвола формалізовано як скінченний автомат, адаптований до SDN-середовища. Кожен етап життєвого циклу з'єднання, включно зі встановленням, передаванням даних і завершенням, однозначно відповідає діям над таблицями потоків Open vSwitch. Ці дії охоплюють створення нового правила, його оновлення, вилучення запису та налаштування відповідних тайм-аутів. Прототип досліджено у віртуалізованому середовищі KVM [4] з використанням сценаріїв нормального трафіку та трафіку атаки. Експериментальні результати продемонстрували підвищення точності блокування небажаних з'єднань порівняно зі статичними ACL, скорочення часу реакції на інциденти та зменшення ризику для площини керування й каналів взаємодії за прийнятних накладних витрат на обробку пакетів.

Література

1. IBM. What Is Software-Defined Networking (SDN)? | IBM. URL: https://www.ibm.com/think/topics/sdn (date of access: 03.12.2025).
2. Ryu SDN Framework. URL: https://ryu-sdn.org/ (date of access: 03.12.2025).
3. Open vSwitch. URL: https://www.openvswitch.org/ (date of access: 03.12.2025).
4. Interactive cybersecurity training system based on simulation environments / D. Tymoshchuk et al. Measuring and computing devices in technological processes. 2024. No. 4. P. 215–220. URL: https://doi.org/10.31891/2219-9365-2024-80-26 (date of access: 30.11.2025).