УДК 004.891.2

ПЕРСПЕКТИВИ ВИКОРИСТАННЯ ДИНАМІЧНИХ ПРОТОКОЛІВ КЕРУВАННЯ VLAN - МЕРЕЖАМИ У ХМАРНИХ СЕРВІСАХ

Сідлецька Д.Р., магістр. *e-mail: kbm221_sdr@student.ztu.edu.ua*
Єфіменко А.А., к. т. н. *e-mail: yefimenko.andrii@ztu.edu.ua*
Кручинський Я.Т., ст. викл. *e-mail: kkik_kyat@ztu.edu.ua*
Вакалюк Т.А., д. пед. н. *e-mail: kik_vta@ztu.edu.ua*
Державний університет «Житомирська політехніка»

Актуальність та постановка проблеми. З розвитком хмарних технологій підіймається все більше питань про захист та оптимізацію хмарних сервісів. Кожен потенційний користувач хмари обирає тип хмарного сервісу, який буде задовольняти їх потреби. Існують компанії, яким не підходить публічна хмара тому, що вони не можуть відмовитись від використання фізичного обладнання зовсім. Тому компанії обирають собі у користування приватні хмари, або як альтернативу гібридні, виходячи зі своїх потреб.

Безпека хмари тісно пов’язана з використанням віртуальних машин та віртуально локальних мереж. Якщо користувач зупиняється на приватній хмарі, то необхідно фізично відокремити мережу, яка буде утворювати дану хмару, оскільки це є важливим з міркувань експлуатації та безпеки. Хмари використовують одну із форм віртуальних мереж для абстрагування фізичної мережі та створення пулу мережевих ресурсів. Одна з форм віртуальних мереж це VLAN. Мережі VLAN не призначені для хмарної віртуалізації чи безпеки, і їх не слід розглядати самі по собі як ефективний засіб контролю безпеки для ізоляції мереж [1]. Але у приватній хмарі для захисту віртуальних машин, що розташовані на одному або кількох фізичних серверах, використання мережі VLAN буде ефективним.

Основні матеріали дослідження. Віртуальні мережі мають суттєві відмінності від фізичних мереж. Дані мережі працюють у фізичних мережах, але абстракція дає можливість глибоко модифікувати поведінку мережі так, щоб мати вплив на безпеку багатьох технологій та процесів [2].

Віртуальна локальна мережа визначає широкомовний домен, у якому лише ті вузли, що згруповані в кластері, можуть обмінюватися повідомленнями за бажанням. Магістральне з’єднання, яке використовується між інфраструктурою VLAN, може забезпечити дуже високий рівень безпеки з великою гнучкістю. З вище зазначеного можна зробити висновок, що VLAN підтримує багато функцій хмарних сервісів, зокрема масштабованість, безпека і використання віртуальних машин. Фактично комутатори підтримують віртуалізацію пристроїв як на рівні 2 (канал даних) моделі OSI, так і на рівні 3 (мережевий рівень) [3].

Для того, щоб коректно працювала віртуально локальна мережа, необхідно, щоб в базі даних фільтрації (Filtering Database) знаходилась інформація про членство в VLAN. Дана інформація потрібна для прийняття правильного рішення (переслати або відкинути) при передачі кадрів між портами комутатора [4].

Динамічна конфігурація VLAN дає можливість для визначення членства в мережі спираючись на характеристики використовуваних пристроїв, а не місця розташування їх порту комутатора. На основі протоколу GVRP (GARP VLAN Registration Protocol) встановлюється членство в динамічних VLAN на магістральних інтерфейсах комутаторів. Зазначений протокол GARP (Generic Attribute Registration Protocol) застосовується для реєстрації та скасування реєстрації атрибутів, таких як VID. Даний протокол GVRP створює та

розповсюджує динамічно записи про нову реєстрацію в VLAN (Dynamic VLAN Registration Entries). Записи, що динамічно розповсюджуються містять в собі інформацію про зареєстровані на порту VLAN та зміну їх переліку при зміні топології мережі. Ці записи створюються, оновлюються і видаляються в процесі роботи протоколу GVRP. Для активізації роботи протоколу GVRP на портах комутатора використовуються його керуючі елементи, а також для зазначення того, чи ця VLAN може бути зареєстрована на порту.

Висновок. Захист віртуальних машин від будь-якого витоку даних або несанкціонованого доступу є одним із головних обов'язків хмарних провайдерів. При використанні приватної хмари відповідальність лягає на користувача, за правильно налаштовану інфраструктуру, мережу, доступ до інфраструктури тощо.

Для великих підприємств, яким підходить тільки приватна хмара і які своєю чергою досить швидко масштабуються, буде досить зручним використання саме динамічних протоколів VLAN - мереж. Адже вони дають можливість для збільшення ефективності, зменшення часу на оновлення конфігурацій вручну та налаштувань, уникнення помилок які зумовлюються людським фактором та багато іншого.

Хоча на даний час динамічні VLAN не застосовуються широко, в цьому є перспектива та розвиток. Особливо з розвитком хмарних технологій та перенесенням більшості ресурсів компаній, державних установ та маленьких підприємств у хмару. З кожним днем цифра тих, хто переходить у хмару росте і досить з великою прогресією. Незважаючи на це, велика кількість компаній не може ще відмовитись від використання фізичного обладнання, і хоча темпи переходу у хмару є досить значні, відмова від фізичного обладнання станеться не скоро.

Список використаних джерел:

1. «Віртуалізація хмарної мережі: переваги SDN над VLAN» [Cloud Network Virtualization: Benefits of SDN over VLAN] Офіційний пресреліз CSA [Cloud Security Alliance(CSA) Official Press Release]/CSA. - 2021. - Режим доступу: https://cloudsecurityalliance.org/blog/2021/06/25/cloud-network-virtualization-benefits-of-sdn-over-vlan/

2. Cloud Security Alliance's Security Guidance for Critical Areas of Focus in Cloud Computing v4.0/CSA. - 2021.- Режим доступу до ресурсу: https://cloudsecurityalliance.org/download/securityguidance-v4/.

3. Сіраццi Ф., Краснов А. «Хмарна безпека: реалізація віртуалізованої VLAN (V2LAN)» [Sirazzi F., Krasnov A. Cloud Security: A Virtualized VLAN (V2LAN) Implementation] / Міжнародна конференція з питань взаємодії людини і комп'ютера[International Conference on Human-Computer Interaction] - 2016. - Режим доступу до ресурсу: https://www.researchgate.net/publication/304107988_Cloud_Security_A_Virtualized_VLAN_V2LAN_Implementation

4. Воропаєва К. А. Статичні та динамічні VLAN-мережі. Взаємодія однорангових VLAN-мереж. "Інформаційне суспільство: технологічні, економічні та технічні аспекти становлення (випуск 53)" : Міжнародна наукова інтернет-конф., 6–16 листопада 2020 р. – Тернопіль, 2020. – С. 20–21. - Режим доступу: https://openarchive.nure.ua/bitstream/document/13956/1/Voropaeva_20_21.pdf

5. Гунько М.А. Особливості побудови хмарних брандмауер-систем захисту веб-ресурсів / М.А. Гунько, науковий керівник – к.т.н. Ткачов В.М. // РАДІОЕЛЕКТРОНІКА І МОЛОДЬ У XXI СТОЛІТТІ : Тези доповіді / Харківський національний університет радіоелектроники. — Харків, 2019. — С.145-146.