УДК 004.738

І.В.Сітніков
В.А.Гарнага

ПЕРСПЕКТИВИ ЗАСТОСУВАННЯ СЛУЖБИ БЕЗПЕЧНОГО ПРИГРАНИЧНОГО ДОСТУПУ (SASE)

Вінницький національний технічний університет

Анотація

Проведено аналіз недоліків традиційної мережевої архітектури. Досліджено новітню технологію побудови комп'ютерних мереж – Secure access service edge (SASE).

Ключові слова: традиційна модель, комп'ютерні мережі, SASE, ZTNA.

Abstract

The shortcomings of traditional network architecture are analyzed. The newest technology for building computer networks - Secure access service edge (SASE) - is investigated.

Keywords: traditional model, computer networks, SASE, ZTNA.

Вступ

Служба безпечного приграничного доступу (SASE) - це втілення новітніх стандартів безпеки та хмарної архітектури, в основі якого лежить технологія програмно-визначеної глобальної мережі (SD-WAN) [1]. Ця концепція покликана вирішити проблеми, актуальні для традиційних мереж в умовах, де організації дедалі більше покладаються на хмарні сервіси та віддалених працівників. SASE пропонує уніфіковану платформу, що поєднує передові принципи оптимізації мереж, засоби безпеки та обміну даними в хмарі. Таким чином модель забезпечує високу захищеність системи, легкість в управлінні і приємний досвід для клієнтів.

Основна частина

Традиційна модель мережевої архітектури передбачає, що користувачі, де б вони не знаходились, зв'язані у вузли - централізовані центри обробки даних [2]. В рамках традиційної моделі дані і застосунки зберігаються на центральному сервері. Для доступу до цих ресурсів клієнти підключаються до ядра в межах локальної мережі або з допомогою віртуального приватного з'єднання (VPN). Яскраві приклади реалізації традиційної моделі: топології "зірка", "дерево" [3].

Попри простоту і надійність, традиційна модель має недоліки, які відіграють значну роль в умовах широкої популярності хмарних сервісів. Вона не пристосована для вирішення проблем, пов'язаних з безпекою віддалених послуг, таких як Function-as-a-service або Software-as-a-Service. Крім того, вона не здатна забезпечити потреби великої кількості користувачів, які працюють віддалено. В міру того, як окремі функції, застосунки, робочі процеси мігрують у хмару, зростає необхідність фундаментальної зміни підходу до побудови корпоративних мереж.

В моделі SASE механізми управління безпекою знаходяться на периметрі мережі - на стику мережі з хмарою. SASE забезпечує стандартизований набір мережевих інтерфейсів і функцій безпеки, які дозволяють організувати надійне і захищене з'єднання в буферній зоні, тому зникає необхідність примножувати хмарні сервіси, що вимагають індивідуальної конфігурації і керування [4].

SASE передбачає застосування таких технологій:

- програмно-визначена глобальна мережа (SD-WAN): система рішень для розумного керування трафіком між центром і периферійними пристроями [5]. Зокрема, для неї характерне централізоване управління і моніторинг мережі;
- брандмауер як послуга (FWaaS): хмарний сервіс, кластер апаратних міжмережевих екранів, що крім фільтрації трафіку пропонує передовий захист від загроз (ATP), систему запобігання втручанням (IPS), захист DNS та ін [6];
- брокер безпечного доступу до хмари (CASB): точка реалізації політики безпеки між корпоративним користувачем та постачальником хмарних послуг [7]. CASB може поєднувати безліч завдань: від автентифікації клієнтів до шифрування і виявлення шкідливих програм;

- безпечний веб-шлюз (SWG): локальна або хмарна технологія мережевої безпеки, яка забезпечує обмеження трафіку, моніторинг системи та реалізує інші заходи, передбачені корпоративною політикою безпеки [8];
- доступ до мережі з нульовою довірою (ZTNA): концепція, яка полягає в тому, щоб максимально обмежити привілеї користувачів і перевіряти трафік включно з тим, що належить авторизованим співробітникам [9]. В комбінації з попередніми засобами ZTNA дозволяє запобігти зловмисним втручанням і спрощує взаємодію з віддаленими клієнтами, оскільки усуває потребу встановлювати безпечне з'єднання з застосуванням VPN та proxy.

Під час впровадження SASE організації мають враховувати архітектурні чинники, зокрема вибір хмарного провайдера, інтеграція з дата-центрами, доцільність застосування ZTNA та ін. Реальні приклади розгортання SASE демонструють успішну реалізацію в різних галузях - від фінансових послуг до охорони здоров'я, що свідчить про універсальність та адаптивність цієї концепції.

З моменту виникнення моделі в 2019 році безліч компаній встановили SASE ключовим елементом своєї стратегії розвитку. Згідно з дослідженням Aruba Networks 2024 року 59% опитаних заявили про бажання впровадити SASE [10]. Більше того, 69% з них планують завершити перехід протягом наступного року. Ці дані збігаються з опитуванням Axis Security 2023, де 65% учасників повідомили про плани застосувати SASE до 2025 року [11]. Ще 24% проводять відповідні оцінки. З деталями звіту Axis можна ознайомитись на рис. 1.

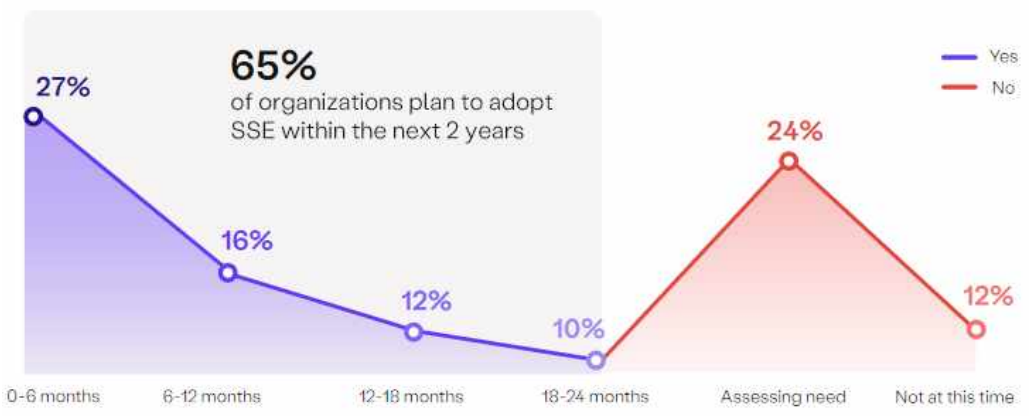

Рис. 1. Графік результатів опитування про SASE.

З огляду на те, що SASE дозволить позбутися багатьох сучасних інструментів безпеки, компанії планують усунути окремі рішення. Їх перелік наведено на рис. 2.

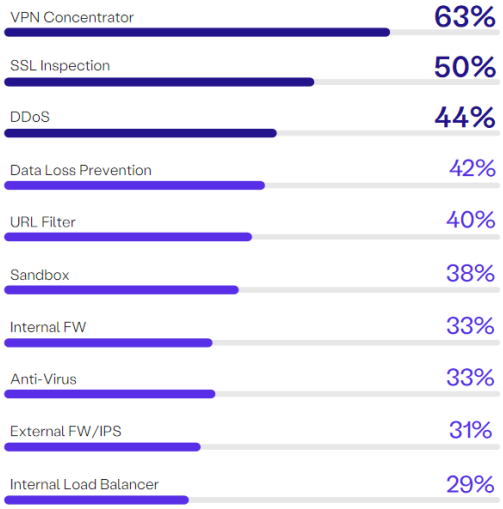

Рис. 2. Результати опитування Axis Networks про зайві інструменти.

Варто звернути увагу на виклики, пов'язані з впровадженням моделі SASE. Розробка принципово нової політики безпеки та застосування новітніх технологій вимагатимуть від спеціалістів глибоких знань та навичок.

У дослідженні Aruba бізнес визначає наступні виклики: забезпечення продуктивності користувачів; застосування ZTNA; підвищення прозорості трафіку; покращення захисту даних; спрощення управління системою; оптимізація робочих процесів для зменшення витрат.

Висновки

У дослідженні проведено аналіз недоліків традиційної архітектури мереж, що знижують її ефективність в умовах широкої популярності віддалених послуг. Зокрема, вона не дозволяє застосувати повний набір функцій, що пропонують сучасні хмарні сервіси і вимагає складні в реалізації рішення для забезпечення безпеки віддалених користувачів.

Проведено оцінку передової моделі SASE, що пропонує інноваційний підхід до управління та захисту мереж. Застосовані технології забезпечують централізоване керування та моніторинг мережі, гнучкий обмін даними з хмарними сервісами. Попри згадані виклики щодо реалізації та новизну запропонованої концепції бізнес зацікавлений у SASE, про що свідчать наведені дослідження.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Yiliyaer S., Kim Y. Secure Access Service Edge: A Zero Trust Based Framework For Accessing Data Securely. *2022 IEEE 12th Annual Computing and Communication Workshop and Conference (CCWC)*, м. Las Vegas, NV, USA, 26–29 січ. 2022 р. 2022. URL: https://doi.org/10.1109/ccwc54503.2022.9720872 (дата звернення: 06.05.2024).
2. Tanguturi R., Bhimini S. The Future of Networking is Here: SASE for a Stronger, More Secure Network. *Journal of Network & Information Security*. 2023. № 11. С. 28.
3. Jackson G. What is network topology?. *IBM*. URL: https://www.ibm.com/topics/network-topology (дата звернення: 25.04.2024).
4. What is SASE architecture? | Secure access service edge. *cloudflare*. URL: https://www.cloudflare.com/learning/access-management/what-is-sase/ (дата звернення: 12.04.2024).
5. SD-WAN - architecture, functions and benefits / P. Segec et al. *2020 18th International Conference on Emerging eLearning Technologies and Applications (ICETA)*, Košice, Slovenia, 12–13 November 2020. 2020. URL: https://doi.org/10.1109/iceta51985.2020.9379257 (date of access: 06.05.2024).
6. CPFirewall: A Novel Parallel Firewall Scheme for FWaaS in the Cloud Environment / Z. Wang та ін. *Lecture Notes in Computer Science*. Cham, 2015. С. 121–136. URL: https://doi.org/10.1007/978-3-319-26979-5_9 (дата звернення: 06.05.2024).
7. Kharb L., Chahal D. Cloud Access Security Brokers: Strengthening Cloud Security. *International Journal of Research Publication and Reviews*. 2023. Т. 4, № 8. С. 642–644. URL: https://doi.org/10.55248/gengpi.4.823.50412 (дата звернення: 06.05.2024).
8. Secure Web Gateway on Website in Cloud / D. Kaur та ін. *Lecture Notes in Electrical Engineering*. Singapore, 2023. С. 19–29. URL: https://doi.org/10.1007/978-981-99-1051-9_2 (дата звернення: 06.05.2024).
9. Bertino E. Zero Trust Architecture: Does It Help?. *IEEE Security & Privacy*. 2021. Т. 19, № 5. С. 95–96. URL: https://doi.org/10.1109/msec.2021.3091195 (дата звернення: 06.05.2024).
10. Security Service Edge Adoption Report. 2024. 23 с. URL: https://www.arubanetworks.com/assets/analysts/2024-SSE-Adoption-Report.pdf (дата звернення: 20.04.2024).
11. Security Service Edge Adoption Report. 2023. 15 с. URL: https://www.arubanetworks.com/assets/analysts/2023-SSE-Adoption-Report.pdf (дата звернення: 20.04.2024).

12. Van der Walt S., Venter H. Research Gaps and Opportunities for Secure Access Service Edge. *International Conference on Cyber Warfare and Security*. 2022. Т. 17, № 1. С. 609–619. URL: https://doi.org/10.34190/iccws.17.1.75 (дата звернення: 06.05.2024).

Сітніков Ігор Володимирович – студент групи 2БС-22б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: thewitness504@gmail.com

Гарнага Володимир Анатолійович – канд. тех. наук, доцент кафедри захисту інформації, Вінницький національний технічний університет, м. Вінниця

Sitnikov Ihor V. – student of group 2BS-22b, Department of Information Technologies and Computer Engineering, Vinnytsia National Technical University, Vinnytsia, e-mail: thewitness504@gmail.com

Harnaha Volodymyr A. – Cand. Sc. (Eng), Assistant Professor of information technologies and computer engineering, Vinnytsia National Technical University, Vinnytsia