ЗАХИСТ МЕРЕЖІ НА ОСНОВІ БРАНДМАУЕРІВ NGFW

Москвін К.С., Севєрінов О.В., Федоров І.А.
Харківський національний університет радіоелектроніки, Харків, Україна

У сучасному світі, де технології стають все більш складними та розповсюдженими, захист мережі стає вкрай важливим завданням для будь-якої компанії або організації. Кількість атак на інформацію, що зберігається, обробляється та передається у мережах постійно зростає [1].

Наступне покоління брандмауерів, так звані NGFW, забезпечують високий рівень безпеки та мають декілька переваг порівняно з традиційними рішеннями [2]. **Метою доповіді є** аналіз принципів роботи засобів NGFW, їх переваги порівняно з традиційними брандмауерами та іншими рішеннями, а також недоліки, які слід враховувати при розгляді вибору захисту мережі.

NGFW працює на основі пакетного аналізу та застосовує цілу низку технологій, таких як DPI (глибокий пакетний інспектор), IPS (система запобігання вторгнень) та VPN (віртуальні приватні мережі), для забезпечення безпеки мережі [3].

Проведений аналіз показав, що NGFW має декілька переваг порівняно з іншими рішеннями захисту мережі. NGFW забезпечує більш високий рівень безпеки мережі, оскільки використовує більш складні технології, щоб виявляти й блокувати небезпечний трафік. По-друге, NGFW має більш широкий функціонал, який дозволяє забезпечити не тільки захист від вторгнень, а й захист від шкідливих застосунків, сайтів та фішингових атак. Також NGFW може обробляти більш великі обсяги трафіку, що дозволяє забезпечити більш високу продуктивність мережі, що в свою чергу забезпечує кращий досвід користувача. NGFW має більш гнучкі настройки, що дозволяє адміністраторам мережі налаштувати правила захисту мережі залежно від потреб організації.

Таким чином, використання брандмауерів NGFW може забезпечити більш глибокий та розширений захист за рахунок використання функцій, таких як контроль доступу до додатків, захист від загроз інтелектуальних атак та більш точні фільтри. NGFW також може бути більш ефективним у виявленні і запобіганні атакам через використання аналізу пакетів та поведінки користувачів.

Список літератури

1. Сєвєрінов О.В., Хрєнов А.Г., Поляков А.О. Аналіз сучасних методів атак на автоматизовані системи управління військами та інформаційні мережі // Системи обробки інформації, 9 (2015). – С. 101-104.

2. Терентьєв О., Горбатюк Є., Лященко Т., Кузьмінський О. Брандмауери нового покоління: дослідження історії розвитку // Управління розвитком складних систем, (45), 2021. – С. 102-106.

3. Гура Д.Ю. Програмний комплекс захисту мережевого периметру інформаційно-комунікаційної системи підприємства, 2021.