УДК 004.85

Івченко О.В., к.т.н., доцент,
Єфименко Д.В., здобувач,
Черкаський державний технологічний університет

РОЗРОБКА ТА ВПРОВАДЖЕННЯ КОМПЛЕКСНОЇ СИСТЕМИ ЗАХИСТУ МЕРЕЖІ НА ОСНОВІ ФАЄРВОЛІВ CISCO НОВОГО ПОКОЛІННЯ (NGFW)

Сучасні корпоративні мережі піддаються зростаючому спектру кіберзагроз, включаючи DoS/DDoS, складні багаторівневі атаки (APT) та експлуатацію 0-day уразливостей[1]. Класичні фаєрволи, що базуються на фільтрації пакетів, є недостатніми для забезпечення належного рівня захисту, оскільки вони не здатні аналізувати трафік на рівні додатків чи протидіяти шифрованим атакам.

Фаєрволи нового покоління (NGFW) [2], зокрема рішення компанії Cisco, поєднують функції міжмережевого екрану, системи запобігання вторгнень (IPS), контролю застосунків та інтеграції з антивірусним захистом.

Об'єктом дослідження в роботі є процеси забезпечення інформаційної безпеки корпоративних мереж. Предметом дослідження є методи та засоби побудови комплексної системи захисту мережі на основі фаєрволів Cisco NGFW (ASA, Firepower).

Мета роботи полягає у розробці та впровадженні комплексної системи захисту корпоративної мережі з використанням фаєрволів Cisco нового покоління, дослідження ефективності їх застосування для протидії сучасним кіберзагрозам.

В результаті виконання роботи було проведено аналіз сучасних кіберзагроз та методів їх нейтралізації. Досліджені функціональні можливості Cisco NGFW (ASA, Firepower Threat Defense – FTD), розроблено архітектуру системи захисту корпоративної мережі на базі Cisco NGFW, налаштувано політики безпеки (контроль доступу, IDS/IPS, фільтрація застосунків, URL-фільтрація). В тестовому середовищі змодельовані типові атаки (SQL-ін’єкції, brute-force, DoS) і оцінена ефективність системи захисту.

Порівняльний аналіз показав, що класичні підходи мають переваги у простоті та низькому впливі на продуктивність, але критично обмежені через відсутність аналізу вмісту трафіку (Layer 7) та неефективність проти сучасних багатовекторних атак.

NGFW (Cisco, Fortinet, Palo Alto, Check Point) [2,3] забезпечують глибоку інспекцію трафіку (DPI), контроль додатків (App-ID),

інтегрований IPS/IDS, SSL/TLS-інспекцію та Sandboxing. Недоліками сучасних рішень є висока вартість та складність налаштування.

Запропонована система захисту побудована на базі Cisco Firepower Threat Defense (FTD) [4], яка об'єднує класичні функції Cisco ASA (міжмережевий екран, VPN) із передовими можливостями NGFW.

Управління системою здійснюється централізовано через Firepower Management Center (FMC), що забезпечує моніторинг, аналітику та інтеграцію із зовнішніми системами SIEM (Security Information and Event Management) та SOC (Security Operations Center).

Проєктування архітектури системи захисту базується на принципах багаторівневого захисту (Defense in Depth) та включає: периметровий NGFW, ізольовану DMZ та захист критичних внутрішніх сегментів.

В рамках практичної частини було розроблено політики доступу, що включають:

• Розмежування прав доступу на основі ролей користувачів та сегментації.

• Реалізація засобів захисту від типових атак: DoS/DDoS захист, захист від SQL-ін'єкцій та інших атак на додатки через інспекцію HTTP/S запитів (WAF), Brute-force prevention: блокування IP-адрес після невдалих спроб аутентифікації.

У тестовому середовищі, що включало сегменти LAN, DMZ, Internet та VPN-клієнтів, було змодельовано атаки (наприклад, сканування портів nmap, SQL-ін'єкції sqlmap) для перевірки ефективності налаштованих IPS-політик та роботи Cisco AMP.

Впровадження комплексної системи захисту на основі Cisco NGFW (FTD) забезпечує багаторівневий захист корпоративної мережі, що є необхідним в умовах сучасних кіберзагроз. Завдяки інтеграції функцій DPI, IPS, AMP та централізованому управлінню через FMC, система демонструє високу точність виявлення загроз та ефективність проти складних шифрованих атак та zero-day експлойтів.

Список використаних джерел:

1. Cisco Talos Intelligence. Threat Research Reports. – Cisco, 2023. – URL: https://talosintelligence.com

2. Anderson, B. Next-Generation Firewall Architectures: Comparative Analysis and Trends // Journal of Cybersecurity. – 2023. – Vol. 12, № 4. – P. 55–72.

3. Sharma, R. Deep Packet Inspection and Application Identification in Modern NGFW Systems // IEEE Security & Privacy. – 2022. – P. 48–57.

4. Cisco Secure Firewall Threat Defense Configuration Guide. – Cisco Systems. – 2024. – URL: https://www.cisco.com