УДК 004.7

Баленко Г. І., здобувач
Дячук О. Ю., ст. викладач
Окунькова О.О., ст. викладач
Державний університет «Житомирська політехніка»

ПІДХОДИ UTM ТА SECURITY FABRIC У ГЕТЕРОГЕННИХ МЕРЕЖЕВИХ СЕРЕДОВИЩАХ: ПОРІВНЯЛЬНИЙ АНАЛІЗ CISCO-РІШЕНЬ ТА OPEN-SOURCE СТЕКУ

Сучасні корпоративні мережі функціонують в умовах стрімкого зростання обсягів трафіку, ускладнення інфраструктур та постійного розвитку кіберзагроз. Використання ізольованих засобів захисту не забезпечує достатнього рівня керованості та швидкості реагування на інциденти, що зумовлює перехід до інтегрованих підходів кібербезпеки. До таких підходів належать концепції Unified Threat Management (UTM) та Security Fabric, які відрізняються архітектурою, рівнем інтеграції та підходами до обробки подій безпеки.

Проблемою дослідження є відсутність узгодженого підходу до інтеграції засобів безпеки у гетерогенних середовищах, що ускладнює централізоване управління та знижує ефективність реагування на інциденти.

Підхід UTM передбачає консолідацію основних механізмів захисту – міжмережевого екрану, VPN, IDS/IPS, фільтрації контенту та контролю застосунків – у межах одного пристрою або програмного вузла. Основною перевагою цього підходу є централізоване адміністрування та спрощене розгортання, однак він має обмеження у масштабованості та гнучкості інтеграції.

На відміну від UTM, концепція Security Fabric базується на взаємодії розподілених компонентів безпеки, що обмінюються телеметрією, подіями та політиками через стандартизовані інтерфейси (API, syslog). Такий підхід забезпечує централізовану кореляцію подій та автоматизоване реагування на інциденти.

У пропрієтарному середовищі ці принципи реалізуються в екосистемі Cisco, зокрема через рішення Cisco XDR, Security Cloud Control, Secure Firewall, Umbrella та Identity Services Engine (ISE). Варто зазначити, що платформа SecureX, яка раніше виконувала роль централізованого рівня інтеграції, поступово заміщується новішими рішеннями, такими як Cisco XDR та Security Cloud Control.

Альтернативою пропрієтарним рішенням є open-source стек, який дозволяє реалізувати подібні функції без значних ліцензійних витрат. До таких компонентів належать:

- **pfSense/OPNsense** – міжмережеві екрани з підтримкою VPN та IDS/IPS;

- **Snort/Suricata** – системи виявлення та запобігання вторгненням;
- **Wazuh** – платформа збору та кореляції подій безпеки;
- **ELK Stack** (Elasticsearch, Logstash, Kibana) – засоби аналізу та візуалізації логів;
- **Ansible** – інструмент автоматизації реагування.

Використання такого стеку дозволяє відтворити ключові принципи Security Fabric, зокрема централізований збір подій, їх кореляцію та автоматизоване реагування.

Аналіз підходів UTM та Security Fabric дозволяє визначити їх принципові відмінності з точки зору архітектури та рівня інтеграції.

UTM реалізує централізовану модель безпеки, у якій функції захисту зосереджені в одному вузлі. Це забезпечує простоту розгортання, передбачувану продуктивність та зручність адміністрування, однак обмежує можливості масштабування та інтеграції з зовнішніми системами.

Security Fabric, навпаки, базується на розподіленій архітектурі, де окремі компоненти взаємодіють через API та механізми обміну подіями. Це дозволяє підвищити рівень автоматизації, забезпечити гнучке масштабування та адаптацію політик безпеки в реальному часі.

У Cisco-рішеннях інтеграція досягається за рахунок єдиної екосистеми, що забезпечує високу узгодженість компонентів. У відкритому стеку інтеграція реалізується шляхом поєднання різних інструментів, що підвищує гнучкість, але ускладнює налаштування.

Таким чином, відмінність між підходами полягає не лише у структурі, але й у рівні автоматизації, масштабованості та можливості інтеграції в багаторівневих системах безпеки.

Для дослідження запропоновано лабораторну модель у середовищах GNS3 або EVE-NG, що включає:

- firewall (Cisco ASA/Secure Firewall або pfSense);
- DMZ-сегмент для генерації трафіку;
- IDS/IPS (Snort або Suricata);
- SIEM-рівень (Wazuh + ELK);
- систему автоматизації (Ansible).

Обмін подіями між компонентами здійснюється через syslog та API.

Передбачено два сценарії:

1. Порівняння UTM-рішень (Cisco vs pfSense/OPNsense);
2. Моделювання Security Fabric у відкритому середовищі.

Для узагальнення результатів аналізу сформовано концептуальну модель очікуваних характеристик досліджуваних підходів.

Таблиця 1

Архітектурне порівняння

Критерій	Cisco	Open-source
Простота розгортання	Висока	Середня
Централізація	Висока	Середня
Гнучкість	Обмежена	Висока
Автоматизація	Висока	Середня–висока
Вартість	Висока	Низька

Таблиця 2

Очікувані метрики

Метрика	UTM	Security Fabric
Продуктивність	Висока	Середня
Latency	Низька	Середня
Час реагування	Середній	Низький
Автоматизація	Середня	Висока

Наведені оцінки мають аналітичний характер і можуть бути використані як основа для подальшої експериментальної верифікації.

Очікуваним ефектом запропонованого підходу є можливість дослідження динаміки поширення подій безпеки між вузлами мережі, аналіз часу реакції системи на інциденти, а також оцінка рівня інтеграції між відкритими та пропрієтарними компонентами в умовах гетерогенного середовища.

Реалізація наведених сценаріїв дозволить:

- сформувати відкрите середовище для тестування концепції Security Fabric без потреби в ліцензіях Cisco;
- розробити навчально-дослідну модель інтегрованої системи безпеки для університетських лабораторій;
- створити методику порівняльного аналізу ефективності open-source і пропрієтарних UTM/Security Fabric систем;
- обґрунтувати доцільність гібридних підходів (Cisco + open-source) у реальних корпоративних середовищах;
- дослідити вплив рівня автоматизації на швидкість реагування на інциденти;
- оцінити ефективність використання SIEM-систем для кореляції подій у гетерогенних архітектурах;
- визначити роль API та NetDevOps-підходів у забезпеченні узгодженої роботи компонентів безпеки.

Перспективи подальших досліджень полягають у проведенні експериментальної оцінки ефективності запропонованої моделі, зокрема:

- вимірюванням продуктивності систем;

- аналізом точності виявлення атак (False Positive/False Negative);
- дослідженням адаптивних політик безпеки на основі автоматизованого реагування;
- інтеграцією моделей машинного навчання для підвищення ефективності виявлення аномалій.

Підхід UTM забезпечує простоту адміністрування та стабільність функціонування, однак поступається підходу Security Fabric у гнучкості інтеграції та рівні автоматизації. Архітектури типу Security Fabric дозволяють ефективніше поєднувати різнорідні компоненти безпеки та реалізовувати адаптивне реагування на інциденти.

Запропонована лабораторна модель створює основу для дослідження інтегрованих систем кібербезпеки у гетерогенних середовищах та може бути використана у навчальному процесі.

У межах проведеного дослідження сформовано аналітичну модель і дизайн експерименту, а практична перевірка запропонованого підходу розглядається як наступний етап дослідження.

Список використаних джерел

1. Siddiqui A., Rimal B. P., Reisslein M., Wang Y. Survey on Unified Threat Management (UTM) Systems for Home Networks. IEEE Communications Surveys & Tutorials. 2024. URL: https://doi.org/10.1109/COMST.2024.3382470
2. Cisco Systems. Cisco XDR – Product Overview. URL: https://www.cisco.com/site/us/en/products/security/xdr/index.html
3. Cisco Systems. Security Cloud Control Firewall Management Documentation. URL: https://www.cisco.com/site/us/en/products/security/firewalls/index.html
4. Cisco Systems. Cisco Secure Firewall Documentation. URL: https://www.cisco.com/site/us/en/products/security/firewalls/index.html
5. Netgate. pfSense Documentation: Remote Logging with Syslog. URL: https://docs.netgate.com/pfsense/en/latest/monitoring/logs/remote.html
6. OPNsense. Intrusion Prevention System (IPS) Documentation. URL: https://docs.opnsense.org/manual/ips.html
7. Wazuh. Log Data Collection Capabilities. URL: https://documentation.wazuh.com/current/user-manual/capabilities/log-data-collection
8. Wazuh. Integration with Network IDS (Suricata). URL: https://documentation.wazuh.com/current/proof-of-concept-guide/integrate-network-ids-suricata.html
9. Chauhan M. A., Babar M. A., Rabhi F. SecDOAR: A Software Reference Architecture for Security Data Orchestration, Analysis and Reporting. arXiv. 2024. URL: https://arxiv.org/abs/2408.12904
10. Davies T., Eiza M. H., Shone N., Lyon R. A Collaborative Intrusion Detection System Using Snort IDS Nodes. arXiv. 2025. URL: https://arxiv.org/abs/2504.16550
11. Pitkar H. Cloud Security Automation Through Symmetry: Threat Detection and Response. Symmetry. 2025. URL: https://doi.org/10.3390/sym17060859