Воротніков В.В., д.т.н., доцент
Мисюк Є.Ю., магістрант
Державний університет «Житомирська політехніка»

ПОРІВНЯЛЬНИЙ АНАЛІЗ ЗАСОБІВ АВТОМАТИЗАЦІЇ ФОРМУВАННЯ СПИСКІВ КОНТРОЛЮ ДОСТУПУ ДЛЯ РІЗНИХ ПЛАТФОРМ МІЖМЕРЕЖЕВИХ ЕКРАНІВ

Списки контролю доступу є основою мережевої безпеки, що забезпечує регулювання доступу до ресурсів через визначення правил для трафіку між сегментами мережі. Вони дозволяють здійснювати гнучке управління доступом, що є критично важливим для організацій з великою кількістю мережевих пристроїв. Однак різноманіття платформ міжмережевих екранів, таких як Cisco ASA, Juniper SRX і Palo Alto Networks, створює значні труднощі в централізованому управлінні політиками безпеки. Це ускладнюється через специфіку форматів списків контролю доступу, різний синтаксис та підходи до їх реалізації.

Основні виклики централізованого управління:

1. Різноманітність платформ: кожна має унікальний синтаксис. Наприклад, Cisco ASA підтримує розширені списки, тоді як Juniper SRX працює із зональними політиками, а Palo Alto Networks орієнтується на додатки.

2. Конфлікти між правилами. У великих мережах дублювання та конфлікти між правилами списків контролю доступу виникають через відсутність узгодженості між платформами. Наприклад, дубльовані правила можуть створити зайве навантаження на міжмережевий екран, знижуючи його продуктивність і ефективність.

3. Обмежені можливості локальних інструментів. Засоби, які надаються виробниками міжмережевих екранів, зазвичай обмежені базовими функціями, такими як створення чи редагування окремих правил. Вони не підтримують автоматизованого аналізу, оптимізації або інтеграції політик між різними платформами.

Сучасні системи автоматизації, такі як Tufin Orchestration Suite, AlgoSec і FireMon, забезпечують ефективне управління політиками безпеки, оптимізацію списків контролю доступу та зменшення ризиків. Ці інструменти мають такі переваги:

• автоматичне виявлення конфліктів між правилами; • оптимізація списків через об'єднання схожих записів; • відповідність стандартам, зокрема ISO 27001.

Tufin Orchestration Suite забезпечує підтримку таких платформ, як Cisco, Palo Alto та Check Point, та дозволяє проводити аналіз ризиків. AlgoSec надає засоби інтеграції політик з хмарними середовищами, такими як AWS, що робить його зручним для гібридних мереж. FireMon фокусується на аналізі прогалин у безпеці, що дозволяє уникнути критичних помилок у налаштуванні.

Згідно з дослідженням [Wool, 2010], автоматизація управління списками доступу дозволяє скоротити дублювання правил на 25–40% та зменшити час на внесення змін до політик безпеки на 50%. Крім того, такі інструменти сприяють підвищенню продуктивності міжмережевих екранів та спрощують їх адміністрування.

Отже, автоматизація формування списків контролю доступу є важливим компонентом забезпечення мережевої безпеки. Інструменти, такі як Tufin Orchestration Suite, AlgoSec і FireMon, допомагають мінімізувати ризики, пов’язані з людськими помилками, та забезпечують ефективне управління політиками безпеки у гетерогенних середовищах. Подальший розвиток цих рішень повинен включати інтеграцію з технологіями штучного інтелекту та підтримку адаптивних політик для динамічних середовищ.

Список використаних джерел

1. Wool A. Trends in Firewall Configuration Errors: Measuring the Holes in Swiss Cheese // IEEE Internet Computing. — 2010. — Т. 14, № 4. — С. 58–65.

2. Al-Shaer E., Hamed H. Discovery of Policy Anomalies in Distributed Firewalls // Матеріали конференції IEEE INFOCOM 2004. — 2004. — С. 2605–2616.