УДК 004.738.5

***Ретивих К.О., магістрант,***
***Колощук М.С., ст. викладач***
*Державний університет «Житомирська політехніка»*

## МОНІТОРИНГ І ВІЗУАЛІЗАЦІЯ МЕРЕЖЕВОГО ТРАФІКУ ЗА ДОПОМОГОЮ ZENARMOR DASHBOARD

Сучасні комп'ютерні мережі постійно зіштовхуються зі зростаючим обсягом трафіку та підвищеною кількістю кіберзагроз. Особливо це ускладнюється тим, що значна частина трафіку передається з використанням протоколу HTTPS і відповідно є зашифрованою, що зрештою ускладнює процес аналізу та виявлення прихованого шкідливого контенту. Ця проблематика вимагає використання технології глибокого аналізу мережевого трафіку, яка часто є ключовою функцією рішень класу Next-Generation Firewall (NGFW), до яких належить і Zenarmor [1].

Метою дослідження є аналіз можливостей системи Zenarmor для моніторингу та візуалізації мережевого трафіку в умовах зростання обсягу зашифрованих даних та кіберзагроз.

Zenarmor позиціонується, як високопродуктивне та гнучке рішення NGFW, розроблене для ефективного протидії сучасним загрозам, особливо прикладного рівня [2]. Ключовою особливістю Zenarmor є його здатність здійснювати глибокий аналіз трафіку і надавати розширені можливості, такі як контроль додатків, веб-фільтрація на основі категорій, аналіз загроз у реальному часі і здійснювати агрегацію та візуалізацію зібраних даних.

В рамках дослідження, з використанням середовища емуляції GNS3, було створено проєкт невеликої локальної комп'ютерної мережі, що складається з робочої станції Windows та маршрутизатора на базі дистрибутива OPNsense зі встановленим плагіном Zenarmor. Zenarmor заздалегідь був налаштований на максимальні безпекові параметри, що включає автоматичне блокування всіх потенційно підозрілих і небезпечних сайтів, недавно створених доменів, азартних ігор, піратських сайтів, соціальних мереж та інших подібних ресурсів.

Для отримання репрезентативного набору даних з браузера робочої станції Windows було здійснено перехід на різноманітні веб-ресурси як дозволених, так і заборонених політиками Zenarmor категорій. Після цього, було переглянуто вкладку зі звітами (Рисунок 1 - ). З цього рисунка можна отримати загальну статистику по розподілу трафіку за загальними категоріями додатків (наприклад Secure Web Browsing чи Media Streaming) і конкретними застосунками (YouTube, Bing, Facebook). Дана візуалізація дозволяє визначити загальний характер

навантаження на мережу й ідентифікувати додатки, які найчастіше використовуються кінцевими пристроями мережі.


Рисунок 1 – Візуалізація розподілу мережевого трафіку за категоріями

На панелі Threats в Zenarmor (рис. 2) можна переглянути загальне співвідношення категорій заблокованих ресурсів (наприклад, Potentially Dangerous, Malware/Virus), тоді як графік праворуч надає інформацію про конкретні домени та URL-адреси (наприклад, fastway01.biz чи itorrents-igruha.org), які були блоковані системою. Це є важливим для швидкого отримання ситуаційної обізнаності та застосування відповідних протидій.

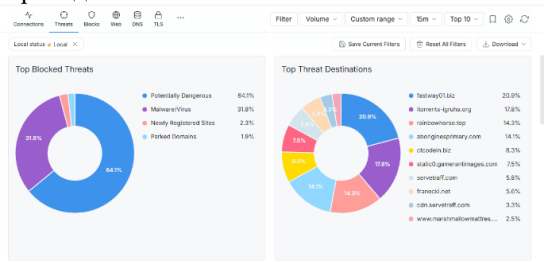


Рисунок 2 – Графічне відображення заблокованих загроз на панелі Zenarmor

Отже, проведене практичне дослідження підтвердило ефективність використання Zenarmor у проактивному захисті мережі від загроз прикладного рівня. Система успішно ідентифікувала та заблокувала ресурси категорій Potentially Dangerous та Malware/Virus, включно з доменами fastway01.biz та itorrents-igruha.org. Панель візуалізації забезпечила зручне групування трафіку як за загальними категоріями (Secure Web Browsing, Media Streaming), так і за конкретними застосунками (YouTube, Bing, Facebook), що дозволяє адміністраторам оперативно оцінювати мережеву активність та приймати обґрунтовані рішення щодо політик безпеки.

**Список використаних джерел:**

1. What is a Next-Generation Firewall (NGFW)? URL: https://www.zenarmor.com/docs/category/ngfw

2. About Zenarmor. URL: https://www.zenarmor.com/docs/opnsense