УДК 004.9

СЕРВІСИ ЗАХИСТУ ВІД DDOS АТАК

SERVICES TO PROTECT AGAINST DDOS ATTACKS

Роман Стецик, Віталій Носов

Харківський національний університет внутрішніх справ, вул. Лесі Українки 30, м. Кам'янець-Подільський, Хмельницька обл., 32301, Україна

***Abstract**. This work examines the most popular services for protection against DDoS attacks.*

Розподілені атаки на відмову в обслуговуванні (DDoS) спрямовані на порушення роботи мережевих сервісів шляхом вичерпання їх ресурсів. Зловмисники синхронно із великої кількості контрольованих вузлів генерують «шкідливий» трафік до об'єкту атаки, що призводить або до погіршення або повного відключення мережевого сервісу [1]. Наразі для повного блокування або пом'якшення DDoS атак створені спеціальні сервіси захисту, які спрямовують, зокрема вебтрафік, у власну мережу, де здійснюється його аналіз на шкідливість та відповідне блокування джерел. Типовий сервіс захисту від DDoS атак фільтрує вебтрафік по геолокації, перевіряє репутацію IP-адрес та пропонує тести CAPTCHA. Аналіз найбільш відомих сервісів захисту від DDoS атак [2] дозволив виділити Cloudflare DDoS Protection, Azure DDoS Protection, Google Cloud Armor та порівняти їх характеристики (табл. 1).

Таблиця 1 – Порівняльна характеристика деяких сервісів для захисту від DDoS атак

Ознака	**Cloudflare DDoS Protection**	**Azure DDoS Protection**	**Google Cloud Armor**
OSI рівні захисту	L3-4, L7	L3-4	L3-4, L7
Показники аналітичного звіту	- масштаб атаки; - атаковані протоколи; - IP адреси та порти, що були під атакою; - час атаки; - загальна кількість байтів яка була заблокована.	- вектори атаки; - статистика трафіку; - причини фільтрації пакетів; - атаковані протоколи; - топ 10 країн або регіонів, з яких йшла атака; - топ 10 мереж (ASN), з яких йшла атака.	- статистика дозволених, відхилених, попередньо дозволених, попередньо відхилених пакетів; - можливість налаштування деталізації статистики.
Мережа	Cloudflare	Microsoft Azure	Google Cloud

З огляду на отримані результати (табл. 1) можна зазначити, що Azure DDoS Protection не забезпечує захист на рівні L7, а у Cloudflare DDoS Protection аналітичний звіт надає більше інформації для реалізації подальших процедур реагування на інциденти кібербезпеки.

Бібліографія

1. Що таке DDoS-атака? URL: https://www.microsoft.com/uk-ua/security/business/security-101/what-is-a-ddos-attack
2. Best DDoS Mitigation Solutions Reviews 2024 URL: https://www.gartner.com/reviews/market/ddos-mitigation-solutions