УДК 621.382

МОДЕЛЮВАННЯ DDoS-АТАКИ НА ВЕБ СЕРВЕР

Лаврів О.А., Колодій Р.С., Хархаліс З.М.
Інститут телекомунікацій, радіоелектроніки та електронної техніки, кафедра «Телекомунікації», Національний університет «Львівська політехніка», Україна
E-mail: zenoviy.m.kharkhalis@lpnu.ua

Мосоров В.Я.
Кафедра комп'ютерних наук в економіці, Лодзький університет, Польща
E-mail: wmosorow@uni.lodz.pl

DDoS-attack on a web server modeling

The main reasons DoS-attack is the most popular attack type in the world are listed. Main features of DDoS-attacks are outlined. The real life case modeling of DDoS-attack on web server was performed. Conclusions drawn from the simulation results are presented.

Атаки типу DoS (Denial of Service), чи радше DDoS (Distributed DoS), є одним з основних типів атак на мережеві ресурси на сьогодні. За даними Лабораторії Касперського, на них припадає близько 6% усіх атак 2015 року (порівняно із 4% у 2014) [1].

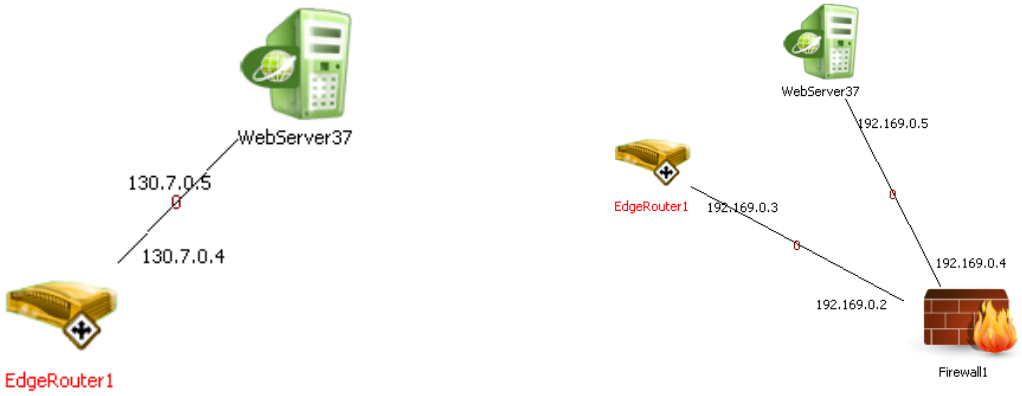
Метою даного дослідження є оцінка ефективності застосування апаратного мережевого екрану для захисту від атак типу DDoS засобами імітаційного моделювання, а також оцінка обсягу необхідних апаратних ресурсів для виконання імітаційного моделювання, яке продемонструє результати, наближені до реальних.

Авторами розглянуто конкретний сценарій DDoS атаки, яка відбулась у 2007 році і була націлена на внутрішню мережу Естонії. Завдяки добре задокументованим фактам [2] вдалось відтворити топологію мережі та провести сплановану DDoS-атаку, параметри і наслідки якої були максимально наближеними до задокументованих.

В загальному випадку, в типовому життєвому циклі атаки виділяють 3 етапи: підготовку, виконання атаки та постфактний період, у якому спостерігаються наслідки проходження атаки. Серед них, етап підготовки є найважливішим та найбільш ресурсозатратним, оскільки вимагає побудови мережі джерел зловмисного трафіку і, що найголовніше, встановлення контролю на цією мережею для синхронного старту атаки і досягнення необхідної для завдання шкоди інтенсивності трафіку. На сьогоднішній день цю проблему вирішують за допомогою т. зв. ботнетів (botnets) [3].

В якості середовища для моделювання вибрано середовище NESSI^2 [4]. Перевагами даної платформи є легкість використання та очевидність представлення в логічному вигляді, де великомасштабні топології можуть мати вигляд однієї іконки. Також було використано можливість платформи автоматично генерувати підмережі із заданими параметрами (напр. за кількістю маршрутизаторів, середньою пропускною здатністю ребер тощо). Середовище

було запущено на відносно слабкій машині з процесором Intel Core Duo T2350 (1.8 МГц), 2 ГБ оперативної пам’яті та ОС Windows Vista.



а) Б)

Рис. 1. Представлені конфігурації: чиста (а) і з мережевим екраном (б).

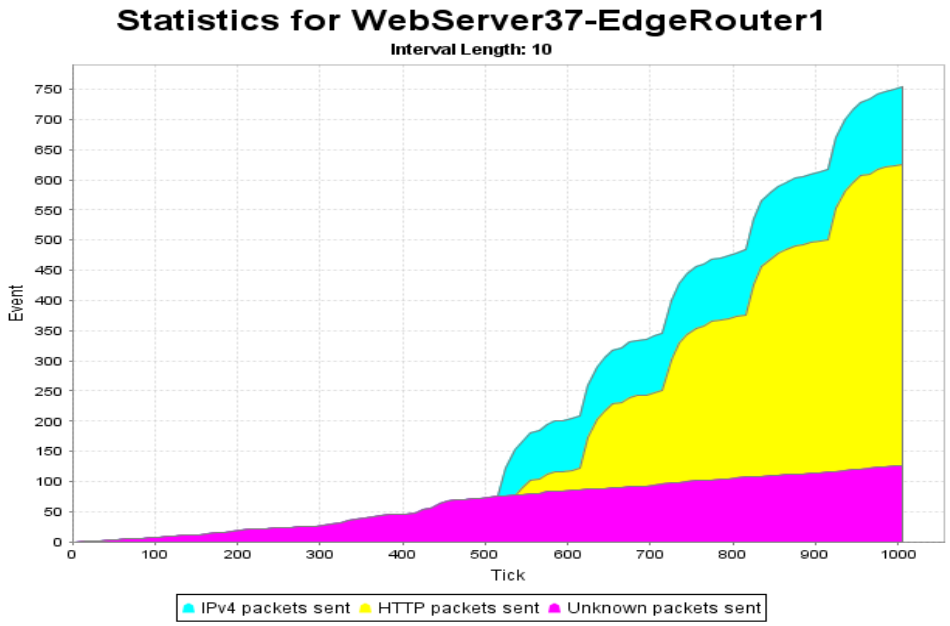


Рис. 2. Атака на веб-сервер без мережевого екрану.

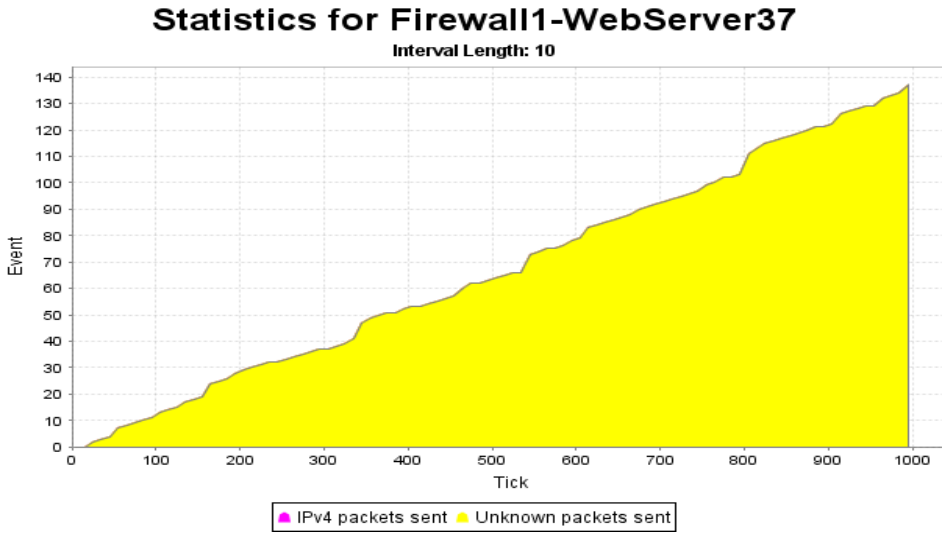


Рис. 3. Атака на веб-сервер з мережевим екраном

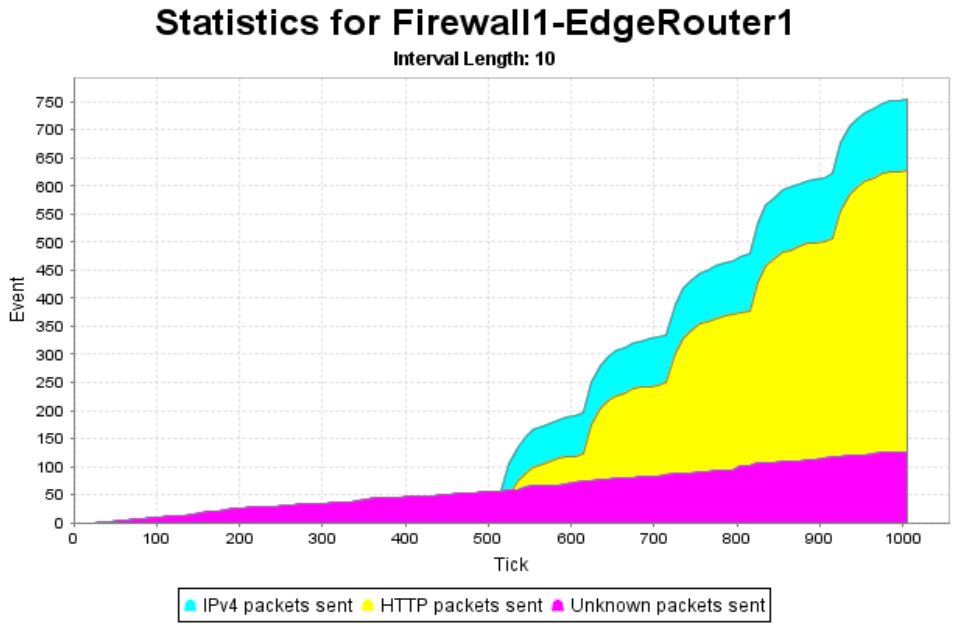


Рис. 4. Внутрішній трафік на мережевому екрані, що захищає веб-сервер

Експериментально визначено, що використовуючи навіть незначні ресурси існує можливість змоделювати доволі масштабну DDoS-атаку, таким чином виділивши слабкі місця у захисті і даючи компетентному персоналу можливість якнайкраще пристосуватись до ймовірних спроб зловмисників завдати шкоди роботі структури.

Порівняно 2 сценарії: змодельовано поведінку трафіку за відсутності та присутності апаратного мережевого екрану між сервером та маршрутизаційною частиною. За наявності мережевого екрану до сервера, що був об'єктом атаки дісталось лише 14% усього шкідливого трафіку, у порівнянні з випадком без екрану (перевантаження у 500%).

Література

1. Юрій Ільїн, Головний редактор Kaspersky Business, Звіт "*IT SECURITY RISKS SPECIAL REPORT SERIES"*, [он-лайн]: https://cdn.press.kaspersky.com/ files/2015/09/ IT_Risks_Survey_Report_Threat_of_DDoS_Attacks.pdf.
2. Merike Kaeo, *"Designing Network Security"*, Cisco Press, oct 30, 2003; [он-лайн]: http:// www.ciscopress.com/store/designing-network-security-9781587051173.
3. Визначення зі словника, [он-лайн]: http://www.dictionary.com/browse/botnet (доступ, травень 2015).
4. Karsten Bsufka and Rainer Bye, *NeSSi² Ver. 2.0.0-beta.3 Manual*, [он-лайн]: http://es.osdn.jp/projects/sfnet_nessi2/downloads/nessi2/2.1.1-beta/NeSSi2Manual.pdf/ (доступ, травень 2015).i