

АНАЛІЗ ВРАЗЛИВОСТЕЙ СУЧАСНИХ МІЖМЕРЕЖЕВИХ ЕКРАНІВ NGFW

Шевчук В.В., Золотарьов В.А.

Харківський національний університет радіоелектроніки, Харків, Україна

Сучасні міжмережеві екрани NGFW (Next-Generation Firewalls) необхідні для захисту мережі від вторгнень, атак та несанкціонованого доступу (НСД). NGFW є еволюційним кроком у розвитку традиційних брендмауерів, оскільки надають ширший спектр захисних функцій, зокрема, детальний контроль за даними, що проходять через мережу.

Метою дослідження є аналіз сучасних міжмережевих екранів вразливостей NGFW.

На сьогоднішній день можна виділити наступні основні вразливості сучасних NGFW такі як: DDoS-атаки (Distributed Denial of Service), внутрішні атаки (Insider Attacks), застаріле програмне забезпечення міжмережевого екрану (Outdated Firewall Software), недоліки активації контролю (Failure to Activate Controls), основні протоколи перевірки (Basic Inspection Protocols), неправильна конфігурація обладнання (Improper Configuration).

Аналіз зазначених вразливостей можна здійснити методом оцінювання ризиків NGFW, який включає: ідентифікацію, аналіз та оцінювання потенційних загроз безпеці міжмережевого екрану.

Аналіз допомагає визначити потенційні небезпеки та вразливості, які можуть виникнути: у наслідку неправильної конфігурації; недоліків в проектуванні; атак з боку зловмисників або інших небезпечних факторів.

Оцінити вразливості вручну практично неможливо в сучасних мережевих середовищах, в яких використовується велика кількість типів NGFW.

Отже слід здійснювати їхню перевірку автоматично і періодично.

Під час оцінювання безпеки NGFW слід перевіряти:

контролювання та керування змінами;

фізичну та програмну безпеку пристроїв;

періодичне покращення правил та очищення застарілих політик;

періодичне проведення оцінювання ризиків і вирішення проблем безпеки мережі.

В результаті проведеного аналізу були визначені основні вразливості NGFW екранів, а також виявлені аспекти оцінки аналізу вразливостей та підвищення безпеки цих екранів.

Список літератури

1. Kamara S., Fahmy S., Schultz E.. Analysis of vulnerabilities in Internet firewalls. 2016. Computers & Security 22(3):214-232: https://www.researchgate.net/publication/222543581_Analysis_of_vulnerabilities_in_Internet_firewalls.

2. Rebecca M, Patrick D., National Institute of Standards and Technology // Guide for Conducting Risk Assessments. – 2012. – №1. – С. 17–22.