УДК 658.51.014

О.С. Гунько,
А.В. Антоненко, д.т.н.
Державний університет телекомунікацій, Київ

МЕРЕЖЕВА БЕЗПЕКА. БРАНДМАУЕР НОВОГО ПОКОЛІННЯ

Коли потрібно захистити мережу, створюються брандмауери, щоб ускладнити зловмисникам доступ до внутрішньої мережі. Брандмауери можуть бути як апаратними, так і програмними. Використовуючи набір правил, брандмауер перевіряє та блокує трафік. Міжмережевий екран може сканувати як вхідний так і вихідний трафік.

У міру розвитку Інтернету їх потрібно було будувати з використанням нових методів безпеки для захисту мережі. Важливо відзначити це в моделі клієнт-сервер, яка є основною архітектурою сучасних обчислень. Мережевий захист, також відомий як брандмауер, можна включити в сучасний пристрій мережевої безпеки організації для включення політики безпеки та керування подіями (SIEM) і встановити на периметрі мережі організації для захисту від зовнішніх і внутрішніх загроз. Коли постачальник виявляє нову загрозу або виправлення, брандмауер оновлює набір правил для адресації постачальника. Основне призначення брандмауера – створити бар'єр між зовнішньою мережею та захищеною мережею. Брандмауер перевіряє всі пакети (фрагменти даних, призначені для передачі через Інтернет), які надходять або залишають захищену мережу. Після того, як інспектор завершить перевірку, брандмауер може відрізнити легітимні пакети від нелегітимних за допомогою попередньо встановленого списку правил. Ця пакетована форма інформації включає джерело, призначення та вміст. Вони можуть відрізнятися на кожному рівні мережі, як і правила. Брандмауери зчитують ці пакети та змінюють їх відповідно до правил, які вказують протоколу надсилати їх туди, куди вони повинні йти.

Брандмауер приймає лише вхідний трафік, на прийом якого він налаштований. Він розрізняє безпечний і зловмисний трафік і дозволяє або блокує певні пакети на основі попередньо визначених правил безпеки. Ці правила базуються на кількох аспектах, які вказують пакетні дані, наприклад джерело, адресат, вміст тощо.

Вони блокують трафік із підозрілих джерел, щоб запобігти кібератакам.

Існує декілька типів міжмережевих екранів залежно від методу фільтрації трафіку, структури та функцій: фільтрація пакетів, брандмауери з проксі-сервером, з перевіркою стану, брандмауери нового покоління.

Брандмауери наступного покоління - це брандмауери з глибокою перевіркою пакетів, які додають перевірку на рівні додатків, запобігання вторгненням та інформацію ззовні брандмауера, на додаток до перевірки та блокування портів/протоколів.

Цей брандмауер забезпечує розширене виявлення та усунення загроз. Співвідносячи мережеві події та кінцеві точки, можна виявити уникнення або підозрілу поведінку.

NGFW покращує фільтрацію пакетів і замість цього виконує глибоку перевірку пакетів (DPI). Подібно до фільтрації пакетів, DPI перевіряє кожен пакет на наявність IP-адрес джерела та призначення, портів джерела та призначення тощо. Вся ця інформація міститься в заголовках пакетів 3-го і 4-го рівнів.

NGFW блокує або дозволяє пакети в залежності від цільової програми; він робить це, аналізуючи трафік на 7-му рівні, рівні додатків. Традиційні брандмауери не мають такої можливості, оскільки вони аналізують трафік лише на рівнях 3 і 4.

ВИКОРИСТАНІ ДЖЕРЕЛА

1.https://www.cloudflare.com/learning/security/what-is-next-generation-firewall-ngfw/

2.https://www.simplilearn.com/tutorials/cyber-security-tutorial/what-is-firewall#:~:text=Firewalls%20prevent%20unauthorized%20access%20to,to%20secure%20a%20computer%20network

3. https://www.cisco.com/c/en/us/products/security/firewalls/what-is-a-next-generation-firewall.html

4. What is a next-generation firewall (NGFW)? | Cloudflare