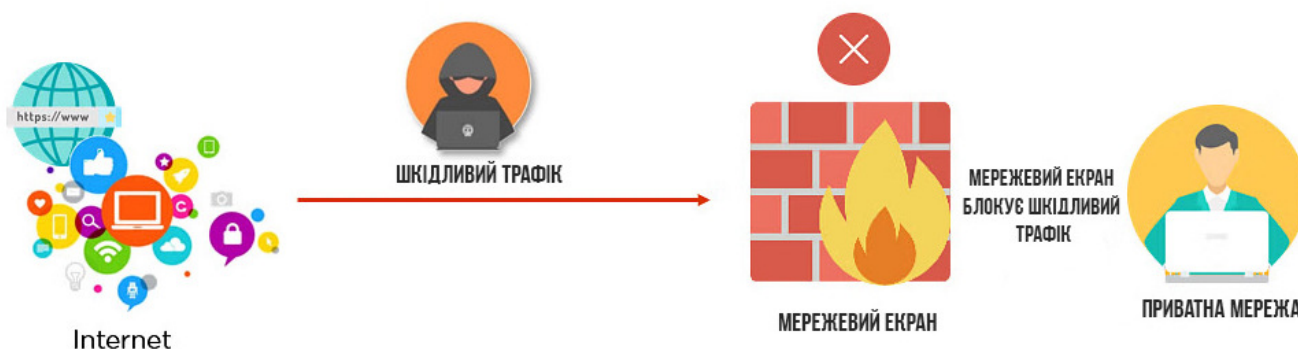


Мережевий екран

Міжмережевий екран, мережевий екран, брандмауер, фаєрв'ол, файрв'ол (англ. Firewall, вогняна стіна) — узагальнювальна назва фізичних пристроїв чи програмних застосунків, сконфігурованих, щоб допускати, відмовляти, шифрувати, пропускати мережевий трафік між областями різної безпеки мережі згідно з бажаним набором правил безпеки.

Це засіб безпеки мережі, який відстежує та фільтрує вхідний і вихідний мережевий трафік, дотримуючись політик безпеки, визначених організацією. По суті, він діє як захисна стіна між приватною внутрішньою мережею та публічним Інтернетом.



Огорожа вашої власності захищає ваш будинок і утримує порушників на відстані; так само брандмауери використовуються для захисту комп'ютерної мережі. Брандмауери — це системи безпеки мережі, які запобігають несанкціонованому доступу до мережі. Це може бути апаратне або програмне забезпечення, яке фільтрує вхідний і вихідний трафік у приватній мережі відповідно до набору правил для виявлення та запобігання кібератакам.

Мережевий трафік

Мережевий трафік або **трафік даних** — це кількість даних, що переміщуються по мережі в певний момент часу. Дані в комп'ютерних мережах здебільшого інкапсульовані в мережеві пакети, які власне і забезпечують навантаження в мережі. Мережа може мати безліч варіантів передачі пакетованого трафіку, але, щоб програми могли розуміти одна одну, трафік створюється відповідно до попередньо домовлених правил, такі правила називаються протоколами мережі, отже, пакетований трафік, який передається відповідно до списку протоколів.

Пакети даних, наприклад, так саме як у випадку з автомобілями на дорозі, можуть мати різний пріоритет, підлягають комутації, маршрутизації, інколи шифруванню, фільтрації вузлами мережі, а по прибуттю, в залежності від правил і протоколів, можуть потребувати перевірки контролю цілісності і джерела надходження. Може виявитись, що передача має втрату пакетів, що вказує на порушення функціонування мережі. Якісні та кількісні характеристики мережевого трафіку є однією із основних характеристик мережі в цілому. Контроль, аналіз, моделювання та управління є запорукою правильного функціонування складних мереж.

- **Аналіз мережевого трафіку** — моніторинг трафіку, його зміни, тенденцій, виявлення атипової поведінки
- **Контроль мережевого трафіку** — управління, встановлення пріоритетів, контроль або зменшення мережевого трафіку
- **Вимірювання мережевого трафіку** — вимірювання кількості та виду трафіку в мережі
- **Моделювання мережевого трафіку** — для вимірювання ефективності комунікаційної мережі
- **Модель генерації трафіку** — це стохастична модель потоків трафіку або джерел даних у комунікаційній комп'ютерній мережі .

Вчасний аналіз та моніторинг мережевого трафіку забезпечує в організації належну безпеку мережі, допомагає вчасно попередити вторгнення у мережу, виявляє потенційні до вразливості вузли мережі.

Типи брандмауерів

Брандмауер може бути програмним або апаратним. **Програмні брандмауери** - це програми, встановлені на кожному комп'ютері, і вони регулюють мережевий трафік за допомогою програм і номерів портів. Тим часом **апаратні брандмауери** - це обладнання, встановлене між шлюзом і вашою мережею.

Сучасні брандмауери часто мають вбудовані додаткові системи безпеки, наприклад віртуальні приватні мережі (VPN), системи запобігання та виявлення вторгнень (IPS/IDS), управління ідентифікацією, управління додатками та веб-фільтрація.

Існує кілька типів брандмауерів залежно від методів фільтрації трафіку, структури та функцій. Кілька типів брандмауерів:

Джерела

- [Мережевий екран](#)
- [What Is Firewall: Types, How Does It Work, Advantages & Its Importance](#)
- [Мережевий трафік](#)

From: <https://library.vpuhluhiv.com.ua/> - **Вікі Глухівського ВПУ**

Permanent link: <https://library.vpuhluhiv.com.ua/subjects:basic:informatika:infsecurity:firewall?rev=1707665497>

Last update: **11.02.2024 17:31**

